Impact of Access Control and Copyright in E-Learning from User's Perspective in the United Kingdom

Galina Akmayeva

A thesis submitted in partial fulfilment of the
requirements of the Brunel University London
for the degree of Doctor of Philosophy

December 2017

Abstract

The widespread adoption of E-Learning has largely been driven by the recommendations of educational technologists seeking to convey the benefits of E-Learning as a valuable accessory to teaching and possible solution for distance-based education. Research in the E-Learning domain has mainly focused on providing and delivering content and infrastructure. Security issues are usually not taken as central concern in most implementations either because systems are usually deployed in controlled environments, or because they take the one-to-one tutoring approach, not requiring strict security measures.

The scope of this research work is to investigate the impact of Access Control and Copyright in E-Learning system. An extensive literature review, theories from the field of information systems, psychology and cognitive sciences, distance and online learning, as well as existing E-Learning models show that research in E-learning is still hardly concerned with the issues of security. It is obvious that E-learning receives a new meaning as technology advances and business strategies change. The trends of learning methods have also led to the adjustment of National Curriculum and standards. However, research has also shown that any strategy or development supported by the Internet requires security and is therefore faced with challenges.

This thesis is divided into six Chapters. Chapter 1 sets the scene for the research rationale and hypotheses, and identifies the aims and objectives. Chapter 2 presents the theoretical background and literature review. Chapter 3 is an in-depth review of the methods and methodology with clear justification of their adaptation and explains the underlying principles. Chapter 4 is based on the results and limitations obtained from the six case studies observations supported with literature review and ten existing models, while Chapter 5 is focused on the questionnaire survey. Chapter 6 describes the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF) and the mapping of the threats from the Central Computing and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM) to Annualised Loss Expectancy (ALE). Chapter 7 presents the conclusions and recommendations, and the contribution to knowledge with further development plans for future work.

List of Publications

2017

1. Akmayeva, G., Ghinea, G., (2017). “E-Learning User’s Authentication”. In the Proceedings of the 12th International Conference on Internet Technologies and Secured Transactions, Cambridge, UK.

2. Akmayeva, G., Ghinea, G., (2017). “Users' Perception of E-Learning Security”. Online Information Review Journal. Emerald Insight. Pending Review.

2011

1. Ayodele, T, Shoniregun, C.A., Akmayeva, G., (2011). 'Towards e-learning security: A machine learning approach', in the Proceedings of the International Conference on Information Society (i-Society 2011), June 27-29, 2011, London, UK.

2. Ayodele, T., Shoniregun, C.A., Akmayeva, G.A., (2011), “Security Review of Email Summarization Systems”, in the Proceedings of the World Congress on Internet Security (WorldCIS 2011), February 21-23, 2011, London, UK.

2010

1. Akmayeva, G., Shoniregun, C., (2010). “Ontology of e-Learning security”, In the Proceedings of the International Conference on Information Society (i-Society 2010), Technically Co-Sponsored by IEEE UK/RI Computer Chapter, London, UK.

2009

1. Chan, Y.T., Shoniregun C.A., and Akmayeva, G.A., (2009). “Applying Semantic Web and User Behavior Analysis to Enforce the Intrusion Detection System”, in the Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST-2009), November 9-12, 2009, London, UK.

2008

1. Chan, Y.T., Shoniregun C.A., and Akmayeva, G.A., (2008). “The memory protector against malicious code attack”, in the Proceedings of the 3rd International Conference for Internet Technology and Secured Transactions (ICITST-2008), 23 - 28 June 2008, Dublin Institute of Technology, Dublin, Ireland.

2. Lin, D., Shoniregun, C.A., and Akmayeva, G.A., (2008). “The VoIP Security in Web2.0 Environment”, in the Proceedings of the International Conference for Internet Technology

and Secured Transactions (ICITST-2008), June 22–25, 2008, Dublin, Ireland.

3. Dannan,L., Shoniregun,C.A., and Akmayeva, G,A., (2008). “The softphone security” in the Proceedings of the IEEE, The 3rd International Conference on Digital Information Management (ICDIM-2008), 13 – 16 November 2008, London, U.K.

Dedication

I dedicate this research work to God Almighty for giving me the strength to accomplish my ultimate goal in life and to those most precious: my Family, my Mother, late Father, Grannies and Grandfathers.

Acknowledgements

My sincere gratitude to Professor George Ghinea for his supervisions, expert guidance and help in providing stimulating and remarkable comments on my research works.

Table of Contents

Abstract II

List of Publications III

Dedications V

Acknowledgements VI

Table of Contents VII

List of Figures XI

List of Tables XIII

Chapter 1: Introduction 15

1.1. Research Rationale 16
1.2. Research Hypothesis 17
1.3. Conceptual Research Context 17
1.3.1. Security Issues in E-Learning 18
1.4. Research Questions 20
1.5. Research Aims and Objectives 20
1.6. Research Plan 21
1.7. Thesis Structure 23
1.8. Summary of Chapter One 24

Chapter 2: Theoretical Background and Literature Review 25

Introduction 25
2.1. Overview of E-Learning 25
2.1.1. Why E-Learning? 27
2.2. Types of E-Learning 31
2.3. Classification and Taxonomy of E-Learning 35
2.3.1. Synchronous E-Learning 37
2.3.2. Asynchronous E-Learning 39
2.4. Current E-Learning Applications 40
2.4.1. Usability of E-Learning 42
2.5. Virtual Communities in Education 43
2.6. Benefits of E-Learning 46
2.7. Challenges of E-Learning 47
2.7.1. Inefficient Online Learner Support 47
2.7.2. Connectivity/ Access Issues 48
2.7.3. Economic Factors – Affordability 48
2.7.4. Untrustworthy Learners 48
2.7.5. Technological Issues 49
2.8.6. E-Learning Vulnerabilities 49
2.9. E-Learning and Security Requirements 51
2.9.1. Identification and Authentication 53
2.9.2. Authorisation 53

2.9.3. Confidentiality 54
2.9.4. Integrity 54
2.9.5. Non-repudiation/Non-denial 54
2.9.6. Availability 55
2.10. Working Groups on Security Management Standards 55
2.11. Security Threats in E-Learning 59
2.11.1. Cross Site Scripting (or XSS) 59
2.11.2. Cross-Site Request Forgery (CSRF) 60
2.11.3. Structured Query Language (SQL) injection 61
2.11.4. Stack-smashing Attacks 61
2.11.5. Session hijacking 62
2.11.6. Removal Attacks 63
2.11.7. Geometric Attacks 63
2.11.8. Cryptographic Attacks 63
2.11.9. Protocol Attacks 65
2.12. Copyright 65
2.13. Access Control 69
2.13.1. Discretionary Access Control (DAC) 72
2.13.2. Mandatory Access Control (MAC) 72
2.13.3. Role-Based Access Control (RBAC) 72
2.13.4. Team-Based Access Control (TMAC) 73
2.13.5. Other Access Control Models 74
2.14. Characteristics of Access Control Models 76
2.15. Authentication 77
2.16. Types of Authentication 77
2.16.1. Knowledge-Based Authentication (KBA) 77
2.16.2. Token-Based Authentication (TBA) 79
2.16.3. Biometrics-Based Authentication (BBA) 82
2.16.4. Location-Based Authentication (LBA) 83
2.16.5. Formula-Based Authentication (FBA) 84
2.16.6. Process-Based Authentication (PBA) 84
2.16.7. Risk-Based Authentication (RBA) 85
2.16.8. Digital Signature Authentication 85
2.16.9. Mobile Pattern Authentication 87
2.17. Comparative Analysis of Authentication Types 87
2.18. Classification of Authentications 89
2.18.1. Single-Factor Authentication 90
2.18.2. Two-Factor Authentication 90
2.18.3. Multi-Factor Authentication (MFA) 91
2.19. Authentication Strength 91
2.20. Copyright in E-Learning 92
2.21. E-Learning Applications and Security Vulnerabilities (case of Moodle and Blackboard) 94
2.21.1. Modular Object-Oriented Dynamic Learning Environment (Moodle) 95
2.21.2. Blackboard 98
2.22. Classification and Taxonomy of E-Learning Security Threats 101
2.23. Summary of Chapter Two 103

Chapter 3: Methods and Methodology

Introduction 104
3.1. Research Paradigms 104
3.1.1. Positivism and Interpretivism 104
3.1.2. Deduction and Induction 105
3.1.3. Quantitative, Qualitative and Mixed Research Methods 107
3.1.4. Summary of Research Paradigms 110
3.2. Data Collection Techniques 110
3.2.1. Literature review 111
3.2.2. Questionnaire 111
3.2.3. Pilot Study 113
3.2.4. Sample Size and Method of Selection 114
3.2.5. Case Studies 114
3.2.6. Framework 116
3.3. Summary of Chapter Three 118

Chapter 4. Analysis of Findings

Introduction 119
4.1. Case Studies 119
4.1.1. Case Study Observation A (CSO A University) 120
4.1.2 Case Study Observation B (CSO B College) 121
4.1.3. Case Study Observation C (CSO C University) 124
4.1.4. Case Study Observation D (CSO D University) 126
4.1.5. Case Study Observation E (CSO E University) 128
4.1.6. Case Study Observation F (CSO F University) 132
4.2. E-Learning Models 134
4.2.1. E-Learning Demand-driven Learning Model 135
4.2.2. E-Learning Community of Inquiry Model 136
4.2.3. Learning Objects Model 137
4.2.4. Laurillard Conversational Framework 138
4.2.5. Centre for Studies in Advanced Learning Technology (CSALT) Networked Learning Model 139
4.2.6. Instructional Design Models for E-Learning 140
4.2.7. Anderson and Elloumi’s Model of Online Learning 142
4.2.8. Clark's Model of Instructional Systems Design 143
4.2.9. Association for Educational Communications and Technology (AECT) Model of Instructional Technology 144
4.2.10. International Society for Performance Improvement (ISPI) Model of Human Performance 145
4.2.11. Comparative Analysis of Ten Existing E-Learning Models 146
4.3. Summary of Chapter Four 148

Chapter 5: Questionnaire Survey: Analysis of Security Issues in E-Learning

Introduction 149
5.1. Section 1 of the Questionnaire Survey: General information 150
5.2. Section 2 of the Questionnaire Survey: The impacts of E-Learning on the delivery of your programme(s) 154
5.3. Section 3 of the Questionnaire Survey: Risk assessment model for 158

assessing the risk of E-Learning environment
5.4. Section 4 of the Questionnaire Survey: Contents and Usage 168
5.5. Section 5 of the Questionnaire Survey: Security Measures 172
5.6. Section 6 of the Questionnaire Survey: Social Awareness 180
5.7. Summary of Chapter Five 182

Chapter 6: Dynamic E-Learning Access Control and Copyright Framework (DEACCF)

Introduction 184
6.1. Proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF) 184
6.2. E-Learning Security Threats Risk Assessment Model 194
6.2.1. Qualitative Approach: CRAMM 195
6.2.2. Quantitative Approach: ALE 196
6.2.3. Mapping CRAMM to ALE 197
6.3. DEACCF Validation 197
6.4. Outcomes of Hypotheses 199
6.5. Summary of Chapter Six 200

Chapter 7: Conclusion

Introduction 202
7.1. Research Conclusion 202
7.2. Contribution to Knowledge 204
7.2.1. Identifying the research gap 204
7.2.2. Current state of security issues in E-Learning 205
7.2.3. Analysis of the usability of single and multifactor authentications 205
7.2.4. Analysis of different authentication methods 205
7.2.5. Proposed Dynamic Framework 205
7.3. Integrating DEACCF to Existing E-Learning Systems 206
7.4. Cost Implications and Learner Friendliness 206
7.5. Limitations 207
7.6. Future Work 208

Glossary 209
Appendix A: Security Issues in E-Learning Questionnaire Survey 213
Appendix B: DEACCF Validation Questionnaire 227
Appendix C: Email Template to E-Learning Developers and DEACCF Description 229
References 237

List of Figures

Figure 1. Networked Teacher

Figure 2. Cognitive and Personal Dimension of E-Learning

Figure 3. E-Learning System

Figure 4. Key Elements in E-Learning Usability

Figure 5. E-Learning Vulnerabilities

Figure 6. List of Some Security Concerns in Everyday Life

Figure 7. Core and Secondary Information Security Concepts

Figure 8. Role-Based Access Control

Figure 9. Attribute-Based Access Control

Figure 10. Knowledge Based Authentication

Figure 11. Token-based Authentication for API Requests

Figure 12. USB Token

Figure 13. OTP Generator

Figure 14. Mobile Phone Authentication

Figure 15. Digital Signature

Figure 16. List of Applications

Figure 17. Session Hijacking

Figure 18. Session Fixation Diagram

Figure 19. Types of Vulnerabilities

Figure 20. Timeline of Blackboard Vulnerabilities within Australian University in 2011

Figure 21. Diagrams of Deductive and Deductive Reasoning

Figure 22. Deductive Reasoning Approach

Figure 23. Quantitative Model

Figure 24. Research within Qualitative Studies

Figure 25. Research within Quantitative Studies

Figure 26. Three Major Research Paradigms, Including Subtypes of Mixed Methods Research

Figure 27. Steps in Constructing a Questionnaire

Figure 28. Selection Strategy for Multiple Case Design

Figure 29. Design Cycle

Figure 30. E-Learning Demand-driven Learning Model

Figure 31. E-Learning Community of Inquiry Model

Figure 32. The CSALT Networked Learning Model

Figure 33. Anderson and Elloumi’s Model of Online Learning
Figure 34. Clark's Model of Instructional Systems Design
Figure 35. AECT's Model of Instructional Technology
Figure 36. ISPI's Model of Human Performance Technology
Figure 37. Impacts of E-Learning on Respondents’ Programmes / Training
Figure 38. Top Reasons for not Using the Available E-Learning Tools
Figure 39. Critical Risk Exposures when Using E-Learning Applications
Figure 40. Respondents’ Roles and Critical Risk Exposures when Using E-Learning Applications
Figure 41. A Risk Management Policy within Institutions / or Companies
Figure 42. How Respondents Assess the Risks Involved in Using the E-Learning System
Figure 43. Remote Users’ Authentication
Figure 44. The Ease of Using the E-Learning System
Figure 45. The Respondents’ Trust in Online Resources
Figure 46. The Importance of E-Learning Security in Institutions / or Companies
Figure 47. The Implementation of Security Policy in Relation to E-Learning in the Respondents’ Institutions/ or Companies
Figure 48. The Usage of any other Authentication Method apart from the Password
Figure 49. The Ability of Respondents to Access Resources /or Services Off-campus
Figure 50. Absolute Security is Unattainable
Figure 51. Single-factor Authentication in E-Learning System
Figure 52. Two-factor Authentication in E-Learning System
Figure 53. Proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF)
Figure 54 (a) and (b). Google User’s Specific Location
Figure 55. Screen Shot of Digital Signatures
Figure 56. Screen Shot of Graphic Pattern Recognition
Figure 57. QR Code
Figure 58. Student’s ID with QR Code
Figure 59. E-Learning Security Threats Risk Assessment Model
Figure 60. Screenshot of One of CRAMM’s Analysis

List of Tables

Table 1. Types of E-Learning

Table 2. Classification and Taxonomy of E-Learning

Tables 3. Types of Virtual Communities

Table 4. Characteristics of access control models

Table 5. The main reasons why a user’s digital signature is secure

Table 6. Comparative Analysis of Authentication Types

Table 7. Classification and Taxonomy of E-Learning Security Threats

Table 8. Research Paradigms and Research Methods

Table 9. Comparison of Qualitative and Quantitative Methods

Table 10. Comparative Analysis of Design Science Research Processes

Table 11. Mapping of learning experience onto Method, Technology and Media form

Table 12. Comparative Analysis of the Ten Existing Models

Table 13. Questionnaire survey distribution frequency

Table 14. Respondents from higher educational institutions

Table 15. Respondents' professional roles within the institutions / or companies

Table 16. E-Learning as part of teaching or professional practice

Table 17. Respondents’ involvement in developing E-Learning applications

Table 18. Respondents’ involvement in training people on how to use the E-Learning applications

Table 19. Response of students in higher education

Table 20. Usage of E-Learning as part of the mode of learning by students

Table 21. Adoption of learning approaches by institution/company

Table 22. Types of technology within E-Learning system

Table 23. Cross-tabulation of Question 2 and Question 11

Table 24. Cross-tabulation of Question 2 and Question 13

Table 25. Types of security risks that institutions /or companies are exposed to

Table 26. Quantifying risks in terms of their impact and probability

Table 27. A risk assessment / or management framework for E-Learning applications

Table 28. Cross-tabulation of Question 17 and Question 21

Table 29. Risk improvement measures

Table 30. System of identifying risks

Table 31. Methods are used for managing the E-Learning risks within institution /or company

Table 32. Safety of E-Learning system

Table 33. Cross-tabulation of Question 22 and Question 34

Table 34. Proportion of the overall content that is available on the course website

Table 35. Frequency of accessing the course materials

Table 36. Cross-tabulation of Question 24 and Question 34

Table 37. The respondents’ experience of using the tools in their E-Learning environment

Table 38. The proneness of the learning system to intrusion by attackers

Table 39. The availability of institutions /or companies’ security and privacy policy to the general public

Table 40. The required measures for login

Table 41. Sharing the login details

Table 42. Cross-tabulation of Question 21 and Question 34

Table 43. Types of risks in E-Learning system

Table 44. Addressing the issue of potential loss of users' confidence in the E-Learning system

Table 45. Respondents’ suggestions in relation to the issue of potential loss of users’ confidence

Table 46. Comparative Analysis of the Six Case Study Observations and DEACCAF

Table 47. Comparative Analysis of the Ten Existing Models and DEACCAF

Table 48. Screenshot of analysis of vulnerability threats

Table 49. Vulnerability Threats Values

Table 50. Participants’ Data Findings Based on Telephone Conversion

Chapter 1: Introduction

The Internet has created convenience for individuals, especially in the educational and business sectors. The information, communication and technology (ICT) has contributed immensely to the learning process of learners, giving birth to various electronic ways of learning. Indeed, technology is enhancing every aspect of education, bringing top-notch courses to the world's poorest citizens and reshaping the way all students learn (Scientific American, 2013).

E-Learning has also provided an alternative compared to the traditional/classroom method for information and instructions to be shared across the Internet between the learner and the tutor just with the touch of a button. E-Learning is as powerful and effective as conventional face to face classroom learning under certain situations. Many educational institutions and companies have adopted E-Learning as a promising solution to provide on-demand learning for their students and employees (Zhang and Nunamaker, 2003). Without doubt, there are some benefits of E-Learning which include reducing costs, time and improving performance of learning. The rapid evolution of digital resources such as video, interactive multimedia and new modes of assessment challenges us to develop different tools and E-Learning projects. But in order to make E-Learning a successful concept, security and privacy as essential factors must be taken into consideration. E-Learning systems employ the Internet as a crossroad to obtain all necessary information and knowledge. The sharing of information, collaboration and interconnectivity are core elements of any E-Learning system. Data must then be protected in order to maintain confidentiality, integrity and availability. Protecting against data manipulation, fraudulent user authentication and compromises in confidentiality are important security issues in E-Learning (Bandara et al., 2014). Apart from increasing the level of awareness of security issues in E-Learning, this thesis will discuss the following:

- ✓ A background of security threats in E-Learning.
- ✓ Access Control and Copyright measures in E-Learning.
- ✓ A critical review of the existing E-Learning models in order to understand the limitations of current Access Control and Copyright issues.
- ✓ Develop a Dynamic E-Learning Access Control and Copyright Framework (DEACCF) using multi-factor authentication method with biometrics.

1.1. Research Rationale

The Higher Education Statistics Agency research findings show that the number of distance learning students registered at UK institutions grew from 357,800 in 2015/16, to 469,221 in 2016/17 (HESA, 2017). A survey conducted in 2017 among 5,723 degree-granting institutions of higher education in the United States reveals that over 6.1 million students were taking at least one online course during the fall 2016 term and 39% of current higher education students have taken at least one course online. Moreover, 72% of higher education institutions now say that online learning is a critical part of their long-term strategy (Pop, 2017). Based on federal data from more than 4,700 colleges and universities, more than 6.3 million students in the U.S. – most of whom were undergraduates – took at least one online course in fall 2016, a 5.6 percent increase from the previous year (Friedman, 2018).

The survey outcomes that were presented by the European University Association between October and December 2013 show that 82% of institutions indicated that they offered online learning courses. Moreover, online examinations are likely to become more widely used for all students in all or most disciplines, also for conventionally taught courses (Gaebel et al, 2014). Undoubtedly, educational institutions and companies spend large sums of money to develop custom training modules or obtain commercial closed-source web-based course management suites such as BlackBoard or WebCT (Floyd et al., 2012). Blackboard is the leading provider of learner success-focused technology solutions and services, serving over 16,000 clients across 90 countries reaching 100 million users (Blackboard, 2017). A hugely popular Moodle (Modular Object-Oriented Dynamic Learning Environment), which was released in 2001, has quickly become one of the most popular and successful open source E-Learning suites. Massive Open Online Courses (MOOCs) have been, up until recently, the reserve of top universities. However, over the last few years, MOOCs have been enjoying a surge in popularity with educational institutions and companies that are widely using the E-Learning applications (UNESCO Bangkok, 2014).

Considering the huge costs of designing and maintaining courses and training online, it is not surprising that security has been given relatively a small amount of consideration by its users and providers. In contrast, research has shown that securing traditional or classroom method of learning has been determined by strict and enforced academic requirements. On the other hand, securing E-Learning focuses not only on unauthorised access, but also on securing content, medium of delivery and ensuring ethics on the part of the user.

1.2. Research Hypothesis

Baxter et al. (1988) state that hypothesis should ideally be:

i. Clearly stated, with no ambiguities or vagueness,
ii. Limited in scope so that it is realistically testable,
iii. Consistent with known facts, in practice this means based on literature.

The hypotheses of the research undertaken have been formulated based on the above principles and literature review.

Hypothesis 1:

- Null hypothesis (H_0^1): Access Control is unattainable in the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF)
- Alternative (H_A^1): Access Control is attainable in the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF)

Hypothesis 2:

- Null hypothesis (H_0^2): The proposed Risk Assessment Model is unattainable in securing the Dynamic E-Learning Access Control and Copyright Framework (DEACCF).
- Alternative (H_A^2): The proposed Risk Assessment Model is attainable in securing the Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

1.3. Conceptual Research Context

E-Learning is a combination of learner, faculty, instructor, technical staff, administrative, learner support, and use of the Internet and other technologies (Volery et al., 2000). Without doubt, technology is transforming E-Learning. Companies now report that E-Learning is the second most valuable training method that they use. It is not surprising, given that E-Learning saves businesses at least 50% when they replace traditional instructor-based training with E-Learning, not to mention that E-Learning cuts down instruction time by up to 60% (Pappas, 2013). As global Internet access continues to grow, so does the prospect of students enrolling in online classes (Amant, 2004) and also the challenges faced by virtual learning system providers to support virtual students. Virtual learning providers have to convince would-be students just like any other online consumer that their products (knowledge and tools) and/or services are viable. From the students' standpoints, issues they consider before participating in virtual learning are highly subjective. As E-Learning increases in popularity and reach, more people run online courses and thus need to understand security issues from a user's perspective.

1.3.1. Security Issues in E-Learning

Generally speaking, many developments in the E-Learning arena have been focused on the technicalities of providing and delivering E-Learning content (The Learning Group, 2003; European Commission, 2005), whilst the need for security in the E-Learning system has often been neglected. The role of security in E-Learning is to provide a secure end-to-end session between the student and the institution's E-Learning network (Graf, 2002; Saxena, 2004), where security can be defined in terms of technical mechanisms. For example, this can be illustrated with the implementation of data integrity using data encryption via virtual privacy for organizations using E-Learning (El-Khatib et al., 2003; Davis, 2004). E-Learning systems are accessed and managed via the Internet by thousands of users over hundreds of networks. The Internet can pose security threats such as unauthorized access, hacking/cracking, obtaining sensitive information, altering data and configuration, as well as enabling academic misconduct incidents (Ramim, 2006). This may lead to unauthorized modification and /or destruction of educational assets (Zuev, 2012).

From a student's perspective, the issue of security within an E-Learning system has a different focus. The focus is based on building a sense of security for the purpose of interaction and collaboration. This encompasses the need to provide privacy and trust for students. Moreover, the ability for a student to maintain a 'personal space' is paramount especially when personal information is shared. This is imperative to preserve privacy for students. Trust, on the other hand, is an age-old issue. Trust can be used to denote that something can be trusted. That is, something trusted is something that the users feel safe with and is proven to be reliable. Within an online E-Learning system, trust is vital when physical interaction is denied and when reliance on trusting others virtually is the only option (Karvonen, 1999). A student would feel more confident in interacting and collaborating with others when there are mechanisms in place to create that privacy and trust.

What are the major E-Learning security threats? According to Schneier (2003), a threat is defined as an undesirable event in the system. The following threats can be identified in the E-Learning system: intrusion of unauthorized users into the system, unauthorized change of data, data eavesdropping, denial of system services and many others. It is very important that an E-Learning system must be secured against manipulation. Maleficent users are also a security hazard in normal application scenarios (Graf, 2002).

Security issues are usually not taken as a central concern in most implementations either because systems are usually deployed in controlled environments, or because they take the one-to-one tutoring approach, not requiring strict security measures.

Among the E-Learning security issues, online cheating is another major problem. It should be noted that studies have been conducted showing that online courses have higher cheating rates than face-to-face courses. According to Dick et al. (2002), 24% of their study participants believed that “advances on technology have led to increased cheating”. According to a study carried out by King et al. (2009), 73.6% of students think that it is easier to cheat in an online environment than in a conventional one. Another way of cheating while taking online exams includes someone else other than the registered student to take an online test. Ndume et al. (2008) argue that preventing cheating in online course assessment is much harder than in traditional classrooms and that the secure assessment of online courses requires the improvement of system security, the registration of learners with unique identification, and the overall administration of the online assessment.

Another E-Learning security issue that draws increasing attention is copyright protection. Most administrators and instructors tend to focus on one type of unethical conduct, namely plagiarism (Naude et al., 2006). However, the copyright holders of E-Learning material have a strong interest in protecting their learning material from illicit use and distribution (Graf, 2002). The major drawback for copyright protection in E-Learning is that the copyrighted material must be made available in digital form to the students. Even though a training provider can restrict access to learning material until a student or learner finalises the payment registration, it does not prevent one paying student or learner from redistributing copies of the learning material illegally.

Apart from user privacy protection, it is important to mention content protection. E-Learning content protection is the protection of the integrity and copyright of course materials. Content authentication has been one of the most important issues in E-Learning. Unfortunately, most E-Learning systems do not provide content integrity protection.

It is becoming very important to advance the level of security in E-Learning systems. Hugl (2005) stated that numerous security related technologies are not currently employed in E-Learning systems. One such solution can include biometrics technologies that may potentially become an integral part of E-Learning systems. In contrast, McGinity (2005) pointed out that biometrics have been commonly employed in replacing conventional password systems. However, it is important not to discard password systems, but to integrate them with other authentication methods in order to make the E-Learning system more secure.

In this thesis, the term E-Learning encompasses both Web-based distance education and Web-sites supplementing in-class teaching. Such course sites typically offer downloads of additional reading, online forums, journals, quizzes, and so on. Research in E-Learning is multidisciplinary, combining very different research areas. Some publications focus on the teaching process and pedagogical issues; others address mainly technical issues such as multimedia transmission, storage, indexing, and networking infrastructure; finally, research on project management in (public) universities, educational policies, and syllabus design contribute to the area of E-Learning as well.

1.4. Research Questions

The following leading research questions have emerged and yet remain unanswered:

1. What precisely constitutes security in E-Learning?
2. Is classification and taxonomy of E-Learning security possible?
3. What constitutes the failure of E-Learning technologies?
4. Is learning content secure when using E-Learning?
5. Is there any risk assessment model that can be used to assess the possible risk incurred by E-Learners?

1.5. Research Aims and Objectives

The research aims of the thesis are as follows:

1. To investigate how Access Control and Copyright can enhance security in E-Learning.
2. To develop and validate the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

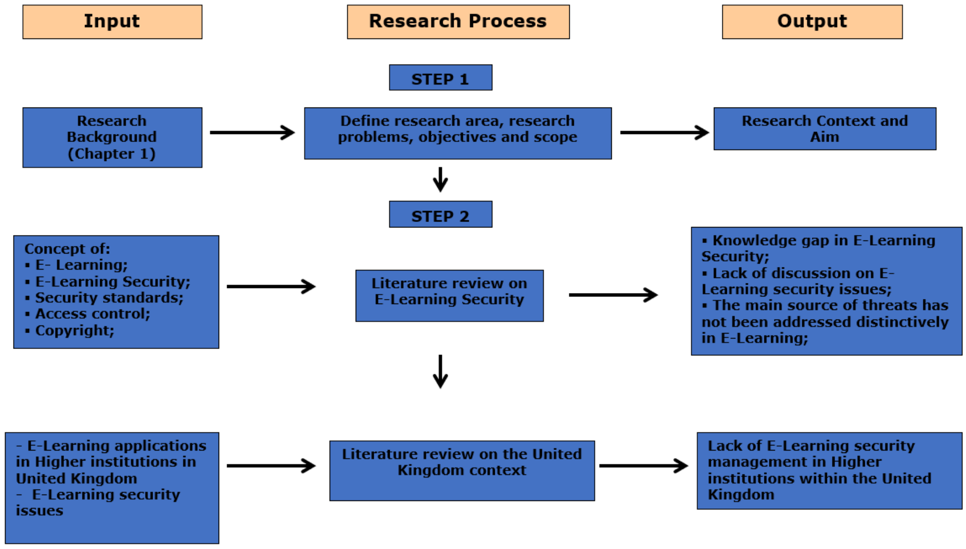
The following objectives have been identified:

Objective 1: To identify what precisely constitute security threats in E-Learning.
Objective 2: To produce a classification and taxonomy of E-Learning security threats that will help in identifying the specific security risks.
Objective 3: To explore Access Control and Copyright measures in E-Learning.
Objective 4: To review the ten existing E-Learning models to
understand the limitations of current Access Control and Copyright issues.
Objective 5: To develop a Dynamic E-Learning Access Control and Copyright Framework (DEACCF) based on the results and limitations obtained from the existing models, case studies observations supported by literature review and questionnaire survey.
Objective 6: To propose multi-factor authentication method and incorporate the E-Learning Security Threats Risk Assessment Model based on hybrid approach that will enhance the security of the Dynamic E-Learning Access Control and Copyright Framework (DEACCF).
Objective 7: To validate the Dynamic E-Learning Access Control and Copyright Framework (DEACCF) by sending a short questionnaire survey to E-Learning developers.

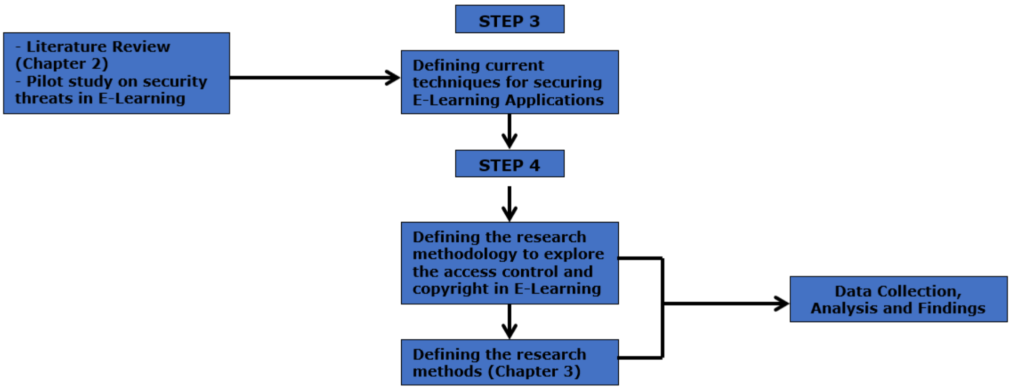
1.6. Research Plan

To have an understanding of the phases and sequences of this thesis, I have outlined the research process in a diagrammatic illustration (see Phases 1-4).

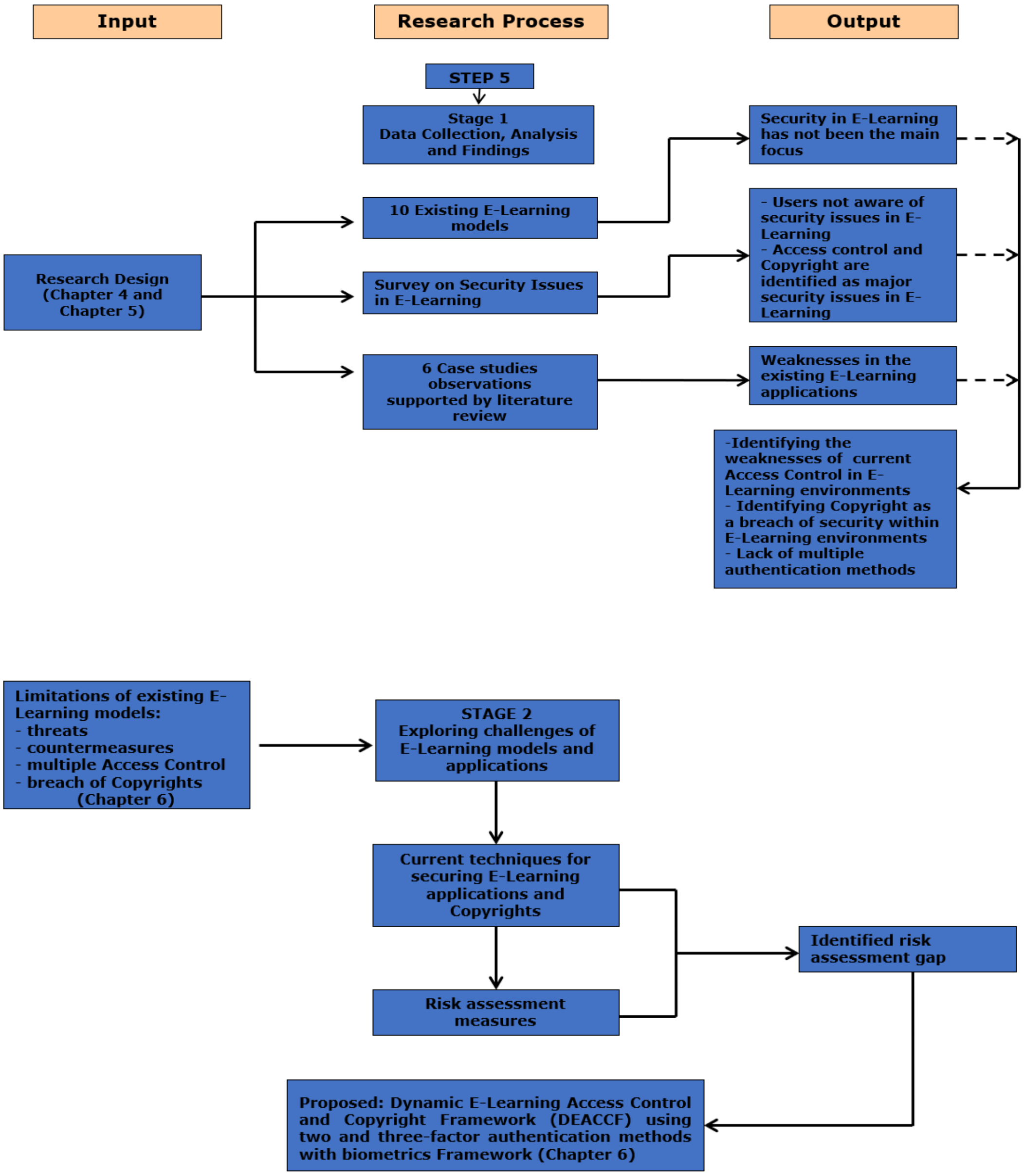
Phase 1


Input
Research Process
Output
STEP 1
Research Background (Chapter 1)
Define research area, research problems, objectives and scope
Research Context and Aim
STEP 2
Concept of:
▪ E- Learning;
▪ E-Learning Security;
▪ Security standards;
▪ Access control;
▪ Copyright;
Literature review on E-Learning Security
▪ Knowledge gap in E-Learning Security;
▪ Lack of discussion on E-Learning security issues;
▪ The main source of threats has not been addressed distinctively in E-Learning;
- E-Learning applications in Higher institutions in United Kingdom
- E-Learning security issues
Literature review on the United Kingdom context
Lack of E-Learning security management in Higher institutions within the United Kingdom

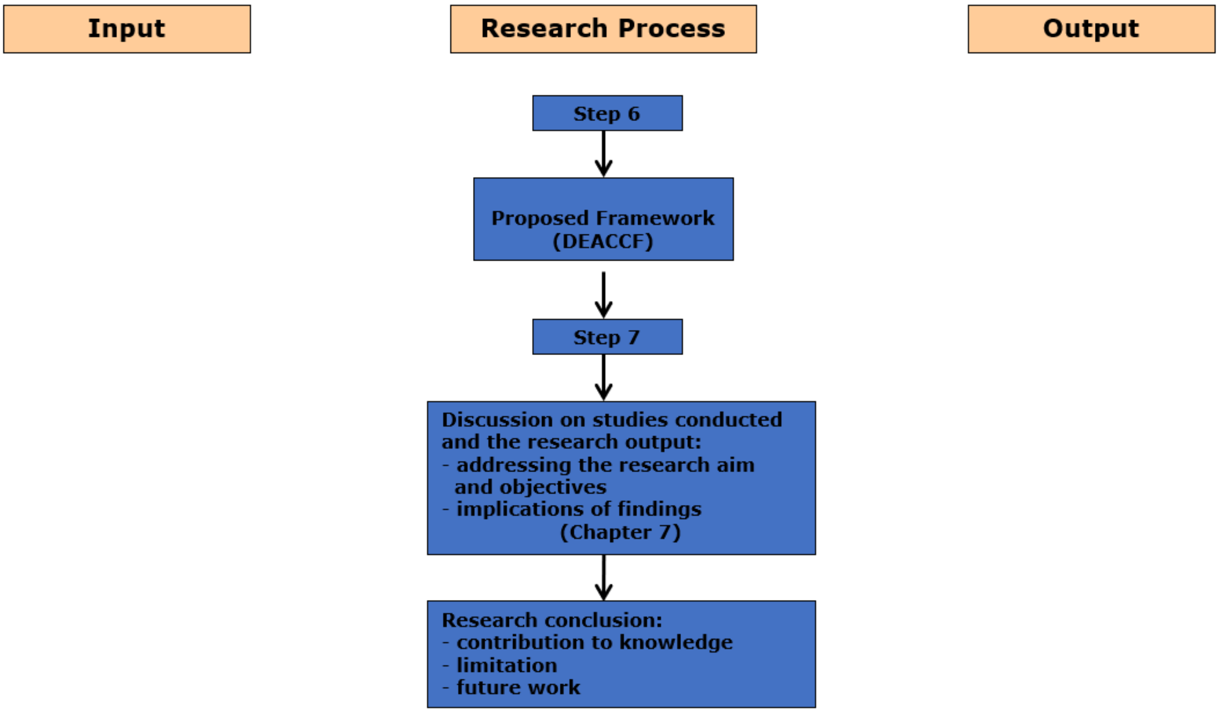
Phase 2


- Literature Review (Chapter 2)
- Pilot study on security threats in E-Learning
STEP 3
Defining current techniques for securing E-Learning Applications
STEP 4
Defining the research methodology to explore the access control and copyright in E-Learning
Defining the research methods (Chapter 3)
Data Collection, Analysis and Findings

Phase 3


Input
Research Process
Output
STEP 5
Stage 1
Data Collection, Analysis and Findings
10 Existing E-Learning models
Research Design (Chapter 4 and Chapter 5)
Survey on Security Issues in E-Learning
6 Case studies observations supported by literature review
Security in E-Learning has not been the main focus
- Users not aware of security issues in E-Learning
- Access control and Copyright are identified as major security issues in E-Learning
Weaknesses in the existing E-Learning applications
-Identifying the weaknesses of current Access Control in E-Learning environments
- Identifying Copyright as a breach of security within E-Learning environments
- Lack of multiple authentication methods
Limitations of existing E-Learning models:
- threats
- countermeasures
- multiple Access Control
- breach of Copyrights
(Chapter 6)
STAGE 2
Exploring challenges of E-Learning models and applications
Current techniques for securing E-Learning applications and Copyrights
Risk assessment measures
Identified risk assessment gap
Proposed: Dynamic E-Learning Access Control and Copyright Framework (DEACCF) using two and three-factor authentication methods with biometrics Framework (Chapter 6)

Phase 4


Input
Research Process
Output
Step 6
Proposed Framework (DEACCF)
Step 7
Discussion on studies conducted and the research output:
- addressing the research aim and objectives
- implications of findings
(Chapter 7)
Research conclusion:
- contribution to knowledge
- limitation
- future work

The follow-up sub-section 1.7. gives an overview of the thesis structure and the content that will be covered within each section.

1.7. Thesis Structure

The thesis is structured as follows:

Chapter 1: This Chapter has set the scene for the research work and conceptual research context.

Chapter 2: This Chapter outlines a literature review and addresses "What precisely constitutes security in E-Learning?" by exploring the conceptual understanding of E-Learning, benefits and challenges, types of E-Learning, classification and taxonomy of E-Learning, security requirements and threats, copyright and access control. In this Chapter we also analyse the current techniques for securing E-Learning applications and Copyrights.

Chapter 3: Methods, methodology and analysis of findings are the main focus of this chapter. We describe the methods and justification, which concerned with the techniques.

The analysis of the findings is the collective results from the questionnaire survey, case study and laboratory experiment.

Chapter 4: This Chapter focuses on the six case study observations supported by literature review and ten existing E-Learning models.

Chapter 5: The results of the questionnaire survey on Security Issues in E-Learning are presented in this Chapter.

Chapter 6: This Chapter is based on the Dynamic E-Learning Access Control and Copyright Framework (DEACCF) using multi-factor authentication methods with biometrics is proposed. The E-Learning Security Threats Risk Assessment Model based on hybrid approach is incorporated to DEACCF to mitigate the Access Control security breaches during and after the user's login.

Chapter 7: Contains a summary of the research findings and outlines the contribution to the knowledge. Finally, the limitations of this research are discussed and directions for future research are proposed.

1.8. Summary of Chapter One

This chapter has set the scene for the research. The direction to which this thesis is going has been made clear and the hypotheses postulated. The E-Learning background and emerging E-Learning tools and applications show that there is a need for security measures in E-Learning.

Chapter 2 contains a literature review, which explains "What precisely constitutes security in E-Learning?" by exploring the conceptual understanding of E-Learning, Benefits and Challenges, Information Security in relations to E-Learning, Legislations, Copyright as security issues in E-Learning and Application Security problems.

Chapter 2: Theoretical Background and Literature Review

Introduction

The last decade has been a resurgence of interest in the training provided by employers. The Internet, apart from being the modern way of getting information, has cut across the education system in a speedy manner. More and more web-based courses and on the job training activities are being arranged on daily basis. Web based learning programmes have made life much easier for learners and workers in some extraordinary ways (Heathfield, 2016). Existing evidence suggests that the UK has maintained a sturdy increase in education regardless of cost. The organization of education and training has been transformed immensely. The competition to recruit and preserve highly skilled workers to improve productivity is on the high rise. The role E-Learning plays in expanding the distance learning market and delivery of overseas courses has been the subject of much recent debate, offering a range of communication tools and content publishing features to facilitate Web-based interaction and content dissemination for low-contact and distance learning students.

The widespread adoption of E-Learning has largely been driven by the recommendations of educational technologists seeking to convey the benefits of E-Learning as a valuable accessory to teaching and possible solution for distance-based education. According to the survey that was conducted by the European University Association between October and December 2013, 82% of institutions indicated that they offered online learning courses. Moreover, online examinations are likely to become more widely used for all students in all or most disciplines, also for conventionally taught courses (Gaebel et al., 2014).

This chapter will answer “What precisely constitutes security in E-Learning?” by exploiting the Conceptual Understanding of E-Learning, benefits and challenges, types of E-Learning (distinctive features and examples of technologies in Synchronous and Asynchronous E-Learning), Information Security in relations to E-Learning, Legislations, Copyright as security issues in E-Learning and Application Security problems.

2.1. Overview of E-Learning

The last decade has seen a significant expansion in E-Learning technologies for enhanced access to education and training. E-Learning is conceptualised in a number of ways. Essentially, it is about the transmission of learning content using information technology and often refers to delivery using intra or Internet. The actual learning which involves identification of information, conceptualising and making meaning to enhance user's knowledge base, understanding and skills, as well as finding the time and space for learning is left to the individual.

Many organisations recognise the benefits of E-Learning because it provides just-in-time, contemporary learning and can be accessed from any site using the right technology (Roffe, 2002). It is seen as a cost-effective approach to facilitating learning to large groups using information and communication technology. The content could be personalised and is embedded in a learner centred framework. Many E-Learning programs are interactive and can be updated rapidly. These and similar benefits were acknowledged in Young's research (2002) on the first major benchmarking study of E-Learning organisations in the United Kingdom. Initial investments in E-Learning are costly, hence the performance, quality, usage, effectiveness and efficiency as a learning solution is of interest to many. However, the current research base, informing evaluation of E-Learning from a wide range of stakeholders or comprehensive return on investment, remains limited. Despite the paucity in this field of research, benchmarking exercises are used by organisations to define a level of performance, and identifying or establishing good practice to improve on that performance (Butson, 2003). According to Dublin (2004), there are six fundamentals to ensure that E-Learning is used by learners and embraced by the organisation. These fundamentals are premised on the understanding that E-Learning is about:

- Business and providing a business solution;
- Providing a "return on expectation", not just a return on investment;
- Enabling learning and driving performance, not training;
- People – learners, managers and executives not technology;
- Motivating learners and energizing organisations; and
- Becoming invisible; interwoven into the very fabric of your organisation and its culture.

The above are familiar to Ettinger et al.'s (2005) research with 29 companies who were E-Learning pioneers. They identified six key factors that underpinned E-Learning:

- Delivering what the business needs
- Putting the learner at the heart of E-Learning
- Providing high-quality content and technology

- Gaining support at senior levels for E-Learning
- Providing pro-active support for e-learners (and their managers) through communication, promotion and marketing
- Creating an organisation that genuinely values learning.

Most organisations implementing E-Learning do so with a view to improving learning services, thereby achieving certain business goals (Ettinger et al., 2005; Dublin, 2004; Roffe, 2002; Young, 2002). These organisations believe that improving learning services improves business outcomes. E-Learning solutions have been known to support strategic outcomes (Fry, 2001). Many educational institutions seek E-Learning solutions to maintain or enhance their market position in a highly competitive environment with declining public subsidy. E-Learning services relate mainly to the management of E-Learning and use electronic media to deliver flexible vocational education and training. It includes access to, downloading and use of web, CD ROM or computer-based learning resources in the classroom, Virtual Learning Environment (VLE), workplace or home. It also includes online access to and participation in course activities (e.g. online simulations, online group discussions), directed use of the Internet for learning and research purposes, structured learning-based email communication and online assessment activities.

2.1.1. Why E-Learning?

The E-Learning cycle has been triggered by technology expectations and technology vendors. It only slumped into a trough of disillusionment when the realities of E-Learning became clear: educators and learners have not adopted E-Learning as expected and desired learning outcomes are not being achieved (Logan, 2001; Taylor 2002; Serdyukov, 2017). In the growth and experimentation phase of E-Learning in the 1990s, universities, public and corporate institutions, incited by technology learning management system vendors, based their E-Learning initiatives on an E-Learning model comprising three elements: service to the customer (learner), content and technology. Owing to the continuous ICT developments, the focus was primarily on the use of technology to create convenient virtual learning environments for learners to access anywhere, any time (JISC, 2016).

Today, E-Learning is being viewed from different concepts such as the Networked Teacher. As the technological environment changes rapidly, it is important to note the current state of technological-based education with regards to giving value to E-Learning (see Figure 1).

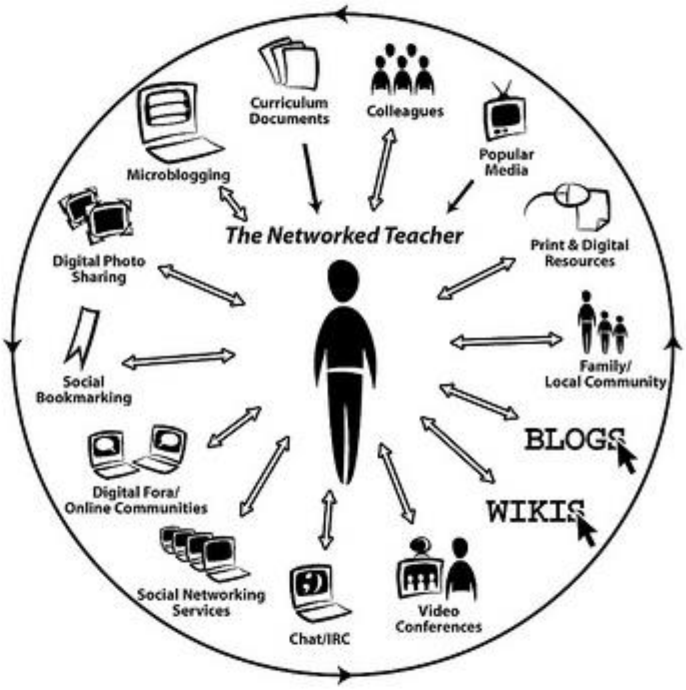


Figure 1. Networked Teacher (Couros, 2010)

The concept of open/distance learning can be used similarly to that of flexible learning. As the term implies, it is based on eradicating physical contact between the tutor and the learner. The learner learns from home rather than attending classes - though some institutional courses require subsequent observation by the tutor. This concept has been adopted from the past and has now moved into more modern methods. In the UK, the Open University was a convention towards the support of this concept. This has enabled learners (especially adult learners) to conquer their learning barriers. Paradoxically, learners with other learning difficulties also gain from this concept in addition to adults. However, technology critics consistently argue for a balanced review of any technology, but the threats, challenges, and losses brought by technology are typically less discussed. While focusing on barriers might be construed negatively, it is not intended to dissuade organizations or individuals from using learning technologies (Alkharang and Ghinea, 2013).

A more technological advanced concept is computer-based training (CBT), which takes the largest adoption in most training organizations today. Taking over instruction delivery for close to three decades now due to already existing computer machines, it subsequently became more advanced especially with the commencement of networking concept and other add-ons such as interactive videos. A typical CBT course would consist of live display of information on a computer screen, in which the user has control of map reading through the course content.

Since the term E-Learning is used inconsistently, it is better to start with a basic definition. E-Learning, at its best, is learning that complements traditional methods and gives a more effective experience to the learner. Simply, E-Learning is the use of technology to support the learning process (The Scottish Government, 2016). Fundamentally, it is about putting the learner first by placing resources at the learner's fingertips. The e-learner is able to dictate the pace and balance of learning activities in a way that suits him/her. E-learners can absorb and develop knowledge and skills in an environment that has been tailored to suit them – and at their own pace.

The Internet is now an educational tool that offers a global open platform for information storage and display in text, graphic, audio and video format as well as communication tools for synchronous and asynchronous interaction (Keegan, 2000). E-Learning in its broadest sense can be defined as instruction delivered via all electronic media including the Internet, intranets, extranets, satellite broadcasts, audio/videotape, interactive TV and CD-Rom. For the purpose of this research work, E-Learning refers to teaching and learning that is web-enabled. Other definitions and terminology of E-Learning are as follows:

> "E-Learning is about information, communication, education and training. Regardless of how trainers categorize training and education, the learner only wants the skills and knowledge to do a better job or to answer the next question from a customer."
>
> - Kelly (2005)

> "E-Learning is the confluence of three social and technical developments: distance learning, computer-conveyed education, and Internet technologies. E-Learning does not change how humans learn, but it does change how we teach them."
>
> - Horton (2000)

> "…instruction that is delivered electronically, in part or wholly via a Web browser, through the Internet or an intranet, or through multimedia platforms such CD-ROM or DVD." Hall argues that, as the technology improves, E-Learning has been identified primarily with using the web, or an intranet's web. Increasingly - as higher bandwidth has become more accessible - it has been identified primarily with using the Web, or an

intranet's web, forcing the visual environment and interactive nature of the web on the learning environment.

- Hall (1997)

"E-Learning refers to the use of Internet technologies to deliver a broad array of solutions that enhance knowledge and performance." Rosenberg claims that E-Learning is based on three fundamental criteria:

- E-Learning is networked, instant updating, storage and retrieval, distribution and sharing of information is therefore possible.
- E-Learning is delivered to the end-user via a computer using standard Internet technologies.
- E-Learning focuses on the broadest view of learning: learning solutions going beyond the traditional paradigms of training.

- Rosenberg (2001)

"E-Learning is forever. Continuous education. The forty year degree. Daily learning. Work becomes learning, learning becomes work, and nobody ever gradates."

- Abernathy (1999)

"The delivery of learning materials, packages or opportunities (i.e. content) through various forms of electronic media, including the Internet, intranets, extranets, satellite broadcast, audio/video tape, interactive TV, and CD-ROM. They use E-Learning synonymously with technology-based learning or TBT.

- Urdan and Weggen (2000)

"Learning that is supported by Information and Communication Technologies (ICT). E-Learning is, therefore, not limited to 'digital literacy' (the acquisition of IT competence) but may encompass multiple formats and hybrid methodologies, in particular, the use of software, Internet, CD-ROM, online learning or any other electronic or interactive media".

- Cedefop (2001)

> "... effective E-Learning as the integration of instructional practices and Internet capabilities to direct a learner toward a specified level of proficiency in a specified competency".
>
> - Conrad (2000)

As the Internet is fast becoming an everyday tool for institutions and companies worldwide, using the Internet for teaching and learning is becoming a normal extension to our social responsibilities and acceptance.

2.2. Types of E-Learning

The main focus in teaching and training is on the learners. For this reason, it is imperative that Learner information be protected from security threats like hackers and identity theft. Learners should have control of their information at all times as a privacy measure. The E-Learning networks, which are likely prone to virus attacks, should have the presence of functional methods such as controlling access, restricting visitation of certain sites, e-mail Spam activation, authorisation and authentication of all activities. Learners should be trained on ethics that would cultivate trustworthy learners and would set a more secured E-Learning system. Table 1 briefly explains the main types of E-Learning.

Table 1. Types of E-Learning

Type of E-Learning	**Description**
Distance Education	**According to Morrison (2014), "distance learning has come a long way since the early days of the Open University. The Internet has made course materials more accessible and contact with tutors easier, and the advent of massive open online courses (MOOCS) created the opportunity to study at a prestigious university for free".**
Virtual Education	**Virtual education is the use of information and communication technologies (ICTs) to deliver educational programs and courses. According to Santelli (2014), "Virtual learning is gaining respect as a viable pedagogical tool thanks to adoption by large institutes and corporations that provide these customisable collaboration spaces and innovative strategies that invite people to learn at their own pace and on their own time".**
Online Education	**Online Education allows the study of higher education courses through the electronic medium of Internet. Course Materials, including reference papers, study materials and contact with tutors and fellow students are all accessed through the use of personal computers and telecommunications. Online Education allows students previously unknown freedom to study at virtually any location and at any pace that can accommodate their other commitments such as work and family. Diploma,**

	undergraduate and master's degrees, the duration of which is a maximum of five years, can be studied at day or night from home, office and even hotel room if you are a frequent traveller (Kearsley, 2000). Kearsley indicated that online learning affords learner's great flexibility in terms of location and duration of study. He also suggests that additional plus is that online courses "are also highly regarded by both the academic and business community." "Simply put, online learning refers to learning and other supportive resources that are available through a computer. The computer prompts the learner for more information and presents appropriate material based on the learner's response." - Carliner (2003) Carliner's definition suggests a "learner to computer" interaction whereas other definitions highlight "online interaction" also historically called "computer mediated communication" (CMC), although this term covers applications beyond instruction (e.g., decision-making in work teams)." Koufman-Frederick et al. (1999) state that "Internet-based work allows collaborators to communicate anytime, from anywhere to any place. People from different parts of a building, state, country, or continent can exchange information, collaborate on shared documents and ideas, study together, or reflect on their own practices."
Distributed Learning	Oblinger et al. (2001) characterise a distributed learning environment as follows: "where the learning environment exists among a dispersed student population, is structured according to learners' needs, and tends to integrate traditional institutional functions (e.g. classroom and library)."
Internet Education	The Internet is the "network of networks" or a global computer connection that allows any user (called a client with an Internet connection) to access information on any other computer that furnishes it (Soler-Labajos and Jiménez-Zarco, 2016).
Computer-Based Training (CBT)	Computer-based training (CBT) refers to the computer-mediated training which was initially imparted via CD-ROMs or DVDs. However, nowadays, these e-trainings or web-based trainings are delivered with the help of the Internet via web browsers (Anastasia, 2015).
Computer-Mediated Communication (CMC)	Computer-mediated communication, for example, through use of a package such as Blackboard or simply by using e-mails (Liu et al., 2008).
Computer-Assisted Instruction	An instruction that used computer or digital device to monitor the learning that takes place and present the instructional material (Hung et al., 2016).
Cyber-Learning	Cyber Learning is an innovative approach to higher education on the Internet. Students take courses from home, office or other convenient locations at times that fit their schedule (Lynch, 2016).
Blended learning and multi-modal instruction	This term is often used when learning takes advantage of the best aspects of in-person or face-to-face interaction and E-Learning technologies (Casebourne, 2017).
Mobile E-Learning (M-Learning)	E-Learning has enormous potential to revolutionize the way education is delivered. The introduction of tablets and dual-core mobile devices will only accelerate that trend going forward. The Mobile technologies (M-Learning) are one of the fastest growing

	technologies in the current IT world. Mobile phone manufacturers and service providers are introducing new models almost every month with new innovations and technologies in those mobile phones. Like mobile phone development, tablet pc are using mobile technologies and many IT related companies have come forward with new innovation and trends in the tablet pc technology (Li, 2010). Companies like Microsoft, Apple, Android, etc., are developing operating systems for the tablet machines with attractive user interface. Google's android are used almost every tablet PC's in market now except some machines like Apple's iPad. So with the help of this mobile technology, E-Learning gets the new shape to develop its technology in mobile phones and tablet PCs platform. With the help of Mobile E-Learning, E-Learning users will get accessibility to reach E-Learning materials at anytime and anywhere they need to learn from E-Learning sources. Mobile E-Learning is especially achieved with the help of cloud computing, because cloud sources are easily able to achieve in anywhere and anytime in any kind of machines like PC, mobile phones, Tablet PCs, PDAs. E-learners can able to use the E-Learning sources from either PC or Mobile phones/Tablet PCs. (Rao et al., 2010). Mobile technologies are creating new ways for students to connect with their course materials, their classes and their colleagues, while also providing new ways to save money, while increasing access, productivity and flexibility (Devine, 2013).
Cloud Based E-Learning	The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service (Johnson, 2013). The Cloud computing is a technology that uses the Internet and central remote servers to maintain data and applications. The Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with Internet access (Kumar Singh, 2016). This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. The Cloud computing is broken down into three segments: "application" "storage" and "connectivity". The name Cloud computing was inspired by the Cloud symbol that is often used to represent the Internet in flowcharts and diagrams. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories (Hanyan, 2012; Timewade, 2018): • Infrastructure-as-a-Service (IaaS): The IaaS is a service provision platform that offers the Cloud vendors storage, hardware, sever and networking components. The maintenance of these hardware resources are maintained by cloud vendors. Usually in this case, the clients using this kind of cloud resources need to pay money only for their needs, and they do not need to pay after their work gets finished. The cloud clients can resize or extend this kind of service from their cloud vendors, so the cloud suppliers resize or ad-hoc the services to their clients based upon the user needs. The IAAS facility is offered with the help of virtualisation. The two different kinds of virtualization are outlined by Kumar and Chelikani (2011): i. Full virtualization: when one system or installed software from one machine can run another entire virtual system by its own emulation in it.

ii. Para virtualization: This is a kind of extension from full virtualizations, but it differs only to enable and run many operating systems at a same time. Amazon Web Services is an example of IaaS. It provides virtual server instance API to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed, it is sometimes referred to as utility computing.

- Platform-as-a-Service (PaaS): PaaS is a service platform that offers the development environment for building, testing and delivering software applications or any other services through cloud without any download or installs applications in cloud user's machine (Al-Jumeily et al., 2010). The PaaS in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer. Force.com, (an outgrowth of Salesforce.com) and Google Apps are examples of PaaS. Developers need to know that currently, there are no standards for interoperability or data portability in the cloud (Holloway, 2010). Some providers will not allow software created by their customers to be moved off the provider's platform.
- Software-as-a-Service (SaaS): SAAS is a service Software, the software is offered to customers through the cloud for almost free or low cost. So the cloud users need not waste huge amount of money licence to use certain software applications. In some cases, certain software applications like excel, the users are even able to access in offline mode, and the data processed in that application are synchronized in cloud once they come to online. In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS is a very broad market. Services can be anything from Web-based email to inventory control and database processing. Because the service provider hosts both the application and the data, the end user is free to use the service from anywhere (Association of Modern Technologies Professionals, 2018).

There are many multi-national companies now offering best cloud computing solutions, like Google, Amazon, IBM, Yahoo, and Microsoft. Google's API is a good example for cloud computing applications; Google offers plenty of software applications with the help of cloud such as YouTube, Google apps, Picasa. A private cloud on the other hand is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services. The Cloud based E-Learning is the technology which is a migration of traditional E-Learning techniques on cloud computing technology to enhance the E-Learning system with numerous provisions to improve

	the learning experience of e-learners (Pocatilu et al., 2010). The following are some of the advantages of implementing Cloud based E-Learning: • Lower costs: E-Learning users need not have high end configured computers to run the E-Learning applications. They can run the applications from cloud through their PC, mobile phones, tablet PC having minimum configuration with Internet connectivity. Since the data is created and accessed in the cloud, the user need not spend more money for large memory for data storage in local machines. Organizations also need to pay per use, so it’s cheaper and need to pay only for the space they need (Al-Jumeily et al., 2010). • Improved performance: the cloud based E-Learning applications have most of the applications and processes in cloud, client machines do not create problems on performance when they are working (Rao et al., 2010). • Instant software updates: E-Learning applications run with the cloud power, the software’s are automatically updated in cloud source. Therefore, E-Learners get updates instantly. • Improved document format compatibility: some file formats and fonts do not open properly in some PCs/mobile phones, while the cloud can enhance E-Learning applications without restrictions to specific formats or fonts. • Benefits for students: students get more advantages through cloud based E-Learning. They can take online courses, attend the online exams, get feedback about the courses from instructors, and send their projects and assignments through online to their teachers (Pocatilu et al., 2010). • Benefits for teachers: teachers also get numerous benefits over cloud based E-Learning. Teachers are able to prepare online tests for students, deal and create better content resources for students through content management, assess the tests, homework, projects taken by students, send the feedback and communicate with students through online forums (ibid). While the Cloud based E-Learning is having numerous advantages, still there are some disadvantages that are associated adaptation of Cloud computing in E-Learning. The major limitations in Cloud based E-Learning technology is security. Security plays a vital role as some of the E-Learning materials are confidential. If the data is stored in cloud, the question of security of this valuable data on unknown cloud servers arises. So the confidential data needs to be encrypted before storage in cloud servers (Ketel, 2014).

2.3. Classification and Taxonomy of E-Learning

The classification and taxonomy of E-Learning is based on existing paradigm of distance education using radio to broadcast lectures, sending lecture notes by post either in paper form or CD and computer-based training (CBT) software in conjunction with the fundamental principles of networking and database. Over the past few years, we have seen evidence of an increasing number of people beginning to understand the concept and the importance of

ICT in learning. Technology and more specifically the Internet have made great progress during the last ten years. As a result of technological evolution, the deliveries of teaching materials and course contents have evolved (see Figure 2).

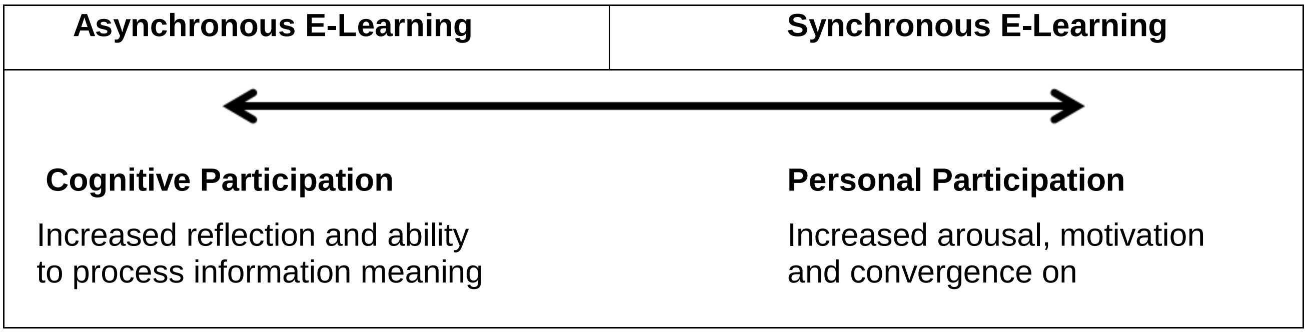

Asynchronous E-Learning
Synchronous E-Learning
Cognitive Participation
Increased reflection and ability to process information meaning
Personal Participation
Increased arousal, motivation and convergence on

Figure 2. Cognitive and Personal Dimension of E-Learning

The continuous transformation in learning value chain systems has led to my proposed classifications and taxonomy of E-Learning, which is presented in Table 2.

Table 2. Classification and Taxonomy of E-Learning

Classification of E-Learning	**Taxonomy**			
	Dimensions	**Distinctive Features**	**Technologies**	**Commonality**
Synchronous E-Learning	Cognitive Participation	• Real-time • Live • Usually scheduled and time-specific • Collective and often collaborative • Simultaneous Virtual presence • Concurrent learning with others • Discussion less complex issues • Getting acquainted • Planning tasks • Students become more committed and motivated because a quick response is expected • Use synchronous means such as videoconferencing, instant messaging and chat, and compliment with face-to-face meetings	• Instant messaging • Online chat • Live Webcasting • Audio conferencing • Video conferencing • Web conferencing/ Webcasting • Games • Cloud	• Multimedia: a mix of text, graphics, animation, audio and video to enhance the learning process; • Interactivity: an instructional strategy that helps a learner practice what they have learned; • Bookmarking: lets the learner stop the course at any time and restart it from the same point; • Report the learner's performance within a course to a Learning Management System (LMS); • Tracking: report the learner's performance

		• Students are expected to work in groups, may be advised to use instant messaging as support for getting to know each other, exchanging ideas, and planning tasks • A teacher who wants to present concepts from the literature		within a course to a Learning Management System (LMS) • Simulation: providing practice with a mock-up of a real system; • Online Experts: provide access to experts through chat or online discussion; • Multiple Bookmarks: designate one or more pages of the course to access while on the job; • Search: search through a course to find information required to complete a task; • Notes and Highlights: mark one or more parts of a course that contain the most important information
Asynchronous E-Learning	Personal Participation	• Intermittent access or interaction • Self-paced • Individual or intermittently collaborative • Independent learning • Usually available anytime • Recorded or pre-produced • Reflecting on complex issues • When synchronous meetings cannot be scheduled because of work, family, and other commitments • Students have more time to reflect because the sender does not expect an immediate answer • Use asynchronous means such as e-mail, discussion boards, and blogs. • Students are expected to reflect individually on course topics may be asked to maintain a blog. • Students are expected to share reflections regarding course topics and critically assess their peers' ideas may be asked to participate in online discussion on a discussion board.	• E-mail • Threaded discussion • Discussion boards and blogs • Web-based training • DVD • Computer-based training • Mobile Phone	

2.3.1. Synchronous E-Learning

Synchronous E-Learning is the traditional instructional approach to online training and has the instructor (or mentor) and learner available at the same time. Usually they are at the same place, but, with the Internet, it is possible for them to be in different places at the same time. Hyder et al. (2007) define Synchronous E-Learning as "live, real-time (and usually scheduled), facilitated instruction and learning-oriented interaction". Synchronous training via the Internet is very helpful for those learners who are willing to adjust their learning style away from the traditional classroom. It is important to identify the main categories of Synchronous and Asynchronous E-Learning technologies. The spectrum of Synchronous and Asynchronous E-Learning technologies and options can appear overwhelming at first. New tools appear with regularity, and existing tools are frequently upgraded or expanded to improve performance and incorporate new features.

The Synchronous learning is live, real-time (and usually scheduled), facilitated instruction and learning-oriented interaction (Hyder et al., 2007). Synchronous E-Learning is synchronous learning that takes place through electronic means. Synchronous learning is distinguished from self-paced asynchronous E-Learning, which students' access intermittently on demand. Synchronous E-Learning has grown rapidly to become a significant component in most organizations and training environments. The following are example of technologies which facilitate Synchronous learning / interaction.

- Audio conferencing can be defined as interaction via telephone. Since audio conferencing is relatively inexpensive and available, most organizations can easily implement synchronous training. Audio conferences are often used in association with other delivery means (such as sending out slides and materials through e-mail, or simultaneous integration with Webcasts and virtual classroom sessions).

- Videoconferencing is a full screen video and audio, either point-to-point or bridged multipoint. Most systems also permit screen sharing and document camera source inputs. Videoconferencing holds great potential for synchronous learning. Its full screen video and high audio quality make it the form that most closely emulates the face-to-face experience and human co-presence. The move from ISDN- to IP-supported videoconferencing has reduced line charges and permitted easier integration with desktop systems. Videoconferencing is well suited to group training split between two or more locations (Hyder et al., 2007).

- Webcasting is utilised for presentation-style, knowledge-dispersal types of learning. Webcasts are typically most practical for reaching large volumes of learners simultaneously, so the opportunities for complex interaction with learners are intentionally restricted. Webcasts can be designed and delivered very quickly and at relatively low costs. Although the video window of a Webcast is typically quite small, the image quality can be very good.

- Gaming and simulations are still in their infancy, but are advancing rapidly and have strong support. Simulations permit participants to learn through practice, and to measure the consequences of actions in a safe context. Games and simulations also promise to facilitate the online learning of psychomotor skills, long regarded as a field of instruction requiring face-to-face demonstration and practice (National Research Council, 2011).

- Web conferencing in particular is used by synchronous virtual classrooms to enhance interactivity and build a sense of community in both online and blended courses (Parker and Martin, 2010). It allows for highly collaborative online learning among geographically dispersed employees. Its interactive architecture is especially well suited to smaller sizes and a facilitative, rather than didactic, teaching methodology. The greatest advantage of Web conferencing is the ability for instructors to present content in a number of different ways, solicit feedback and provide clarification, and then facilitate learner practice and collaborative problem solving (Martin and Parker, 2014).

Despite the growing presence of synchronous E-Learning, there is still uncertainty about how best to plan, design, and deliver for this medium. The field has developed so rapidly that best practices are only now starting to emerge.

2.3.2. Asynchronous E-Learning

Asynchronous E-Learning or Domain means that the training takes place independent of time and relationships. In many cases an instructor (or mentor) is not present for at least part of the time. The learners proceed at their own pace and in their own time. Asynchronous training may include computer-based training, using CD-ROMs, or, more frequently, web-based training, in which a trainee logs into an online training system with a user name and password to begin an interactive course. The course can be easily updated, is accessibly from anywhere and can be used with all kinds of computer systems. The asynchronous environment is most appropriate for those who learn best by thinking about content on their own, and who can structure their time to accommodate instruction.

2.4. Current E-Learning Systems

The E-Learning system consists of E-Learning applications, E-Learning platform and E-Learning environment. The E-Learning Application comprises of many undefined web and cloud based applications that are compatible and interlock with many resources that shared the same E-Learning platform (see Figure 3).

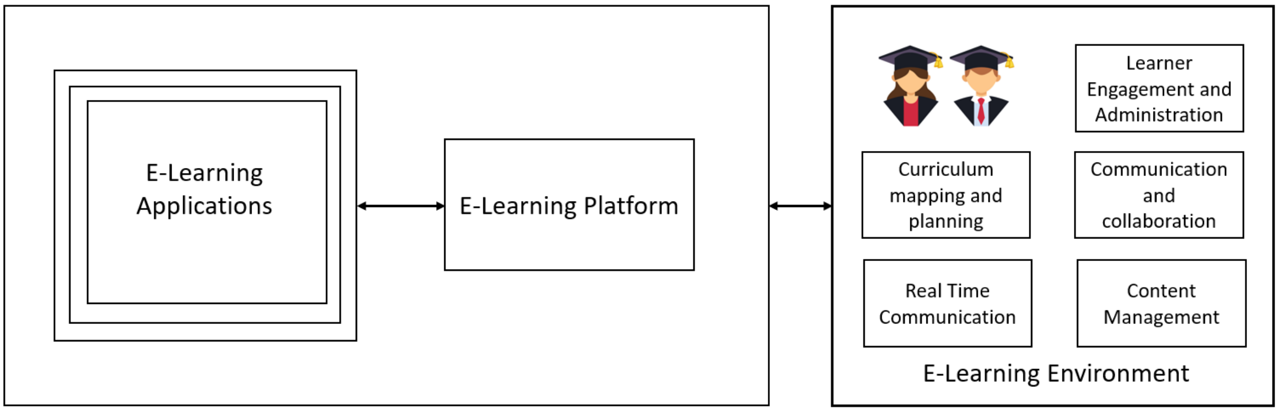


Figure 3. E-Learning System

The E-Learning platforms are generally web-based. They enable the user to access the study materials, take tests, and track their progress whenever or wherever they want. The platforms are generally web-based. It enables the user to access the study materials, take tests, and track their progress whenever or wherever they want. There are many such platforms available in the market. Companies can either use such platforms or develop their own. Developing such platforms may be expensive, so companies generally use already available platforms. The platforms can be free (open source) or commercial. The commercial platforms will let the companies to modify them to fit the needs of the users. While choosing the platform it is necessary for the companies to understand what they want. It depends on a number of factors such as needs of students and technical skills of instructors.

The E-Learning widely uses web-based applications. The web-based applications are designed on multi-tier architectures spanning over multiple boundaries of trust. The vulnerability of a component depends on both platform (Java 2 Platform Enterprise Edition (J2EE) on Tomcat/Apache/Linux, Programming Language (C#) on a Windows .NET server) and the environment (exposed Demilitarized Zone (DMZ) on Local Area Network (LAN)

(Hewett, 2008).

The Web service protocols cannot always be referred to by a simple label like “SOAP over HTTP”, as there exist a huge number of options concerning e.g. cryptographic operations or ways of requesting and passing on security tokens. A similar need for annotation exists with respect to other modelling elements, as trust relationships (Meinecke et al., 2007).

The WebML, OOHDM, UWE and HERA focused on the hypermedia aspect of Web applications from individual pages and navigation nodes rather than a Web-based system’s composition from individual services and applications, while the WebSA applies the model-driven development paradigm by combining architectural models with the design methods mentioned. The WebSA does not suffer from the model to system and system to model problem. Due to the model-driven approach of all the latter applications, there is no integration of security (Ingle and Meshram, 2012).

The Dynamic Systems Initiative (DSI), the Data Center Markup Language (DCML) and the Systems Modeling Language (SysML) have been introduced to close the gap between model and system. DSI is a technological strategy devised by Microsoft that aims at an integrative support for design, deployment and operation of distributed systems (Microsoft, 2003). The initiative is driven by the idea of combining the two processes of building and operating IT solutions to emphasize the application life cycle as a whole. The DSI major focus is on the Windows platform. The Data Center Markup Language (DCML) is an approach that describes data center environments, the dependencies between data centre components and the policies governing management, and construction of those environments. As an application of Extensible Markup Language (XML), it provides a platform-independent specification, and is not restricted to any product but to the context of a data centre. As an example of an approach that tries to merge ideas of an abstract system level, Systems Modeling Language (SysML) focuses on the specification, analysis, design, verification and validation of systems and systems-of-systems based on Unified Modeling Language (UML). The security of all the above approaches is questionable when developing E-Learning systems.

E-Learning systems provide a loosely coupled architecture for building distributed systems with universal interoperability. Some E-Learning systems uses XML to pack data into XML messages defined by SOAP (Simple Object Access Protocol) and also uses XML to describe the data types and services in the SOAP message, called WSDL (Web Service Description Language). Although the E-Learning systems owned by different organizations can be easily integrated; even if they are developed in different programming languages and deployed on different platforms (Middleware/Operating System (OS). The traditional security technologies (Secure Sockets Layer (SSL) and Hypertext Transfer Protocols (HTTPS)) can partially resolve this problem by encrypting messages transferred between two points. Therefore, the point-to-point transport-layer security technologies cannot insure end-to-end security along the entire path in a complicated multi-tiers distributed system. Furthermore, point-to-point security technologies are all based on a specific transport protocol/layer (Transmission Control Protocol (TCP)/ Internet Protocol (IP) for SSL and HTTP for HTTPS) (Tang et al., 2007).

E-Learning environment is at the heart of E-Learning system and it comprises of users, learner engagement and administration (managed access to learner information and resources and tracking of progress and achievement), curriculum mapping and planning (lesson planning and assessment), communication and collaboration (emails, notices, chat, wikis, blogs), real time communication (video conferencing or audio conferencing) and content management (creation, storage, access to and use of learning resources) (see Figure 3).

2.4.1. Usability of E-Learning

Usability testing has long been a part of the software and product design world. Nielsen (1999) brought the concept of usability to the Web, making Web pages simple to navigate and intuitively organised so that users can easily find the information they are looking for. While this definition may be considered sufficient in the world of software, the definition of usability in the E-Learning world should encompass a few more components than simply good user interface design (see Figure 4).

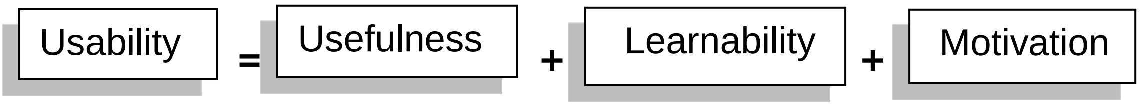


Figure 4. Key Elements in E-Learning Usability

The key elements in E-Learning usability are briefly explained below:

- **Usefulness.** The product not only must be easy to use, but it also should serve a purpose. In the development of E-Learning courses, usefulness is measured as part of the needs assessment for the course - a step that often is rushed because of time and budget constraints. These constraints commonly create a tight relationship between the people conducting the needs assessment and those managing the design and development of an E-Learning course (Adeoye, 2010).

- **Learnability**. Donald Norman, known to many as the authority on workable technology, is the originator of learnability. Learnability is defined as the ease and speed with which users can figure out how to use a product. For example, if learnability is high, users can intuitively learn to use a product without training or manuals. In the world of E-Learning, the definition of learnability should be expanded to include the ability of users to effectively learn and retain the skills and knowledge. The level of learnability in a course is most often associated with the strengths and weaknesses of the instructional design (Nielsen, 1999).

- **Motivation**. The final component of this expanded definition of usability is the concept of motivation. E-Learning that is created with ease-of-use, usefulness and learnability in mind is simple, has high instructional value and is supportive to the learners in their work. However, the elements missing from E-Learning, such as an instructor, student interaction and an actual physical environment, can result in a lack of learner motivation (Berge, 1998).

2.5. Virtual Communities in Education

Community is a word in use since the middle of the 15th century and comes from the Latin words **commune** and **communis**, meaning together, in common, group of people committed to common and shared duties (Corominas, 1987).

One of the emerging technologies that will dramatically impact schools and the quality of education delivered is known as virtual communities. Also called online communities, these networked individuals can share information and ideas freely through the use of the PC, Internet and a host of other technologies becoming widely available. One of the definitions of virtual communities may be the following: virtual communities are online groups of like-minded individuals who utilize the Internet to share ideas, exchange information, and post relevant topics of discussion and use to the members.

Not all types of virtual communities have the same status: the most generic ones impelled by the development of so-called social web – such as diaries or *blogs* with numbers in the order of hundreds of millions, microcommunites like MySpace or YouTube or discussion groups around a theme of common interest – are good examples of the extent to which technological progress enhanced global communicational skills but they also show how difficult it is to think in terms of educational intervention. Jesse Berst, Editorial Director of the ZDNet AnchorDesk, identifies 6 ways that companies and individuals are designing communities on the Internet (Clouse, 2003):

- Homesteads give members space on the web and this allows them to gather in “neighbourhoods” to share information and ideas with other members;
- Special interest groups come together around specialized topics and information;
- Chat rooms enable members to communicate with members using synchronous and asynchronous methods. These are often less formal and often have guidelines of conduct and use;
- Navigation is offered to train individuals to use certain portals or search engines within the community;
- Geography plays a part in the development of virtual communities. Many online communities grow from regional interests and concerns.
- Commercial ventures also make an attempt to develop a community of customers to better provide goods and services as well as to have quick access to market research.

Virtual communities hold great promise for education. One example of a successful online community is Harvey. Harvey is the software which is useful for communities for many purposes. It was developed by Lloyd Tabb and allows students to communicate with other students in the community, allows users such as students, teacher or parents to work from anywhere, supports many schools or a single server, provides an easy way for students to work on an assignment using Harvey on a web page and has many other features. Institutions have now become virtual-institutions. The Internet now fosters educational activities and a lot more is yet to take place. These put together form the surrounding features of E-Learning. The main types of Virtual Communities are outlined in Table 3.

Tables 3. Types of Virtual Communities

Types of Virtual Communities	Description
E-assessment	Assessment is a very important component of any educational setting. Two major forms are distinguished - Summative and Formative assessment. Learning systems can be built

	around the IMS Learning Design Specification to support creation of the learning designs, instantiation with content and the management of the assessment activity in a real learning context (Heinrich, 2005). The E-assessment is the electronic process by which learners' progress and understanding are assessed (Becta, 2006): • diagnostic (to assess current levels of knowledge and understanding in order to target future learning appropriately) • formative (to support and feed back into current learning) • summative (to assess knowledge and understanding at the end of an episode of learning, usually equated with a formal award)." Becta has been working with consultants to develop a tool to help organisations working in the sector to assess their current policies and practice and develop an action plan to move their work forward. The self-assessment tool and action planning facilities are located at a site called 'The Matrix' which has been developed by NCSL and Becta for schools, but will now host a range of self-assessment tools for the learning and skills sector. The learning and skills matrix supports Individuals or groups to carry out self-analysis and use of the action plan produced. According to Pappas (2015) identifies five types of summative assessment: • Online multiple-choice exams. • Online Presentations. • Creating a website or blog. • Learners' online portfolios. • Online group projects. Pappas further explains that "a summative assessment is administered at the end of an E-Learning course, and provides learners with a final grade, in contrast to formative assessment, which identify areas that may need improvement and pinpoint their strengths".
E-registration	With the help of the Internet some institutions provide students with the capability to register semester courses online. Also in registering courses some academic websites are designed to allow learners make secured tuition payments – much convenient but may have some issues regarding security.
E-administration	Student and staff record keeping can now be easily maintained and tracked via the institution's intranet. Technology has made it much easier for administrators and administration departments to carry out their task.
E-library/resources	This has been of great help to students when they carry out their research work, thesis and course works. Learning resources are made available via the institution's website in form of links to resources (such as websites), journals, research papers, articles, and to mention a few (Su and Lee, 2004). Knowledge Tree separates learning materials into primary materials for average learners and additional materials for learners with different learning styles and knowledge. The system uses learning goals, preferences, and knowledge of the individual learner to select the most appropriate learning materials (Tingane et al., 2016; Martin and Connor, 2017).
E-tutoring	Instructions are being directed to learners online. Tutors are left with the duty to maintain and update content on course website. Also, students can collaborate and discuss courses issues with tutors through chat rooms and mailing systems-incorporated in the institution's

	website. E-tutoring can be defined as teaching, support, management and assessment of students on programmes of study that involve a significant use of online technologies. If teaching in online environments (and online learning) is to be successful, staff development is a key factor (TechLearn, 2000). Two areas are particularly crucial in being an effective online tutor: curriculum review for integrating ICT and the management and support of online learners. The core skills of a good tutor are unlikely to change with a different delivery method.

2.6. Benefits of E-Learning

The availability of accurate information may result in efficiency and effectiveness of the E-Learning delivery, as learner professionals will have more time to study learning materials specifically for their benefit rather than collecting information. Based on the literature review and my experience as an E-Learning security expert, the following are the benefits of E-Learning:

- Efficiency: E-Learning will help to increase efficiency and hence decreasing costs by either avoiding duplications or through enhanced communication possibilities between professionals in different E-Learning organisations and through learner's involvement.
- Enhanced quality of care: Efficiency not only reduces cost but also enhances the quality of care through, for example, allowing comparison between E-Learning providers.
- Evidence-based in the sense that the effectiveness and efficiency of interventions are provided by scientific evaluations rather than assumptions.
- Empowerment through availability of knowledge bases for E-Learning. E-Learning records can be made accessible to other institution over the Internet.
- Encouragement of new relationship between E-Learners and E-Learning professionals and, therefore, decisions are made in a shared manner.
- Education of the E-Learning professionals through online resources.
- Enabling information exchange and communication between E-Learning establishments in a standardised manner.
- Extending the scope of E-Learning. Geographical boundaries in the provision of learning are removed through the use of the Internet where E-Learners may easily obtain E-Learning services online from the global providers.
- Equity to have E-Learning more accessible to all.

Claims are often made about the potential improvement in the quality of learning materials and decrease in cost (Twigg, 1999). However, less has been said about security or improvement of access control to E-Learning records and study materials. The latter raises the issue why security in E-Learning is vital.

It is surprising to know that notwithstanding E-Learning benefits, limitations are still present. A significant challenge is security. Despite all the enthusiasm about E-Learning, security issues are holding back many learners from taking part in on-line training. Unfortunately, not all learners and organizations profit from E-Learning. Several potential barriers or limitations to effective E-Learning have been identified, which should be taken into account by organisations and individuals considering E-Learning as well as providers and developers of E-Learning.

In addition, despite the attractiveness of E-Learning, a study in the UK by Knowledgepool (2000) established that E-Learning is still not entirely well established in the work place - even where it is made accessible. In this study, it has been revealed that less than one in five companies had an E-Learning policy. This tends to bring in contradicting questions on the best way to deliver instruction. Some of the existing challenges or limitations of E-Learning are discussed in the sub-sections below.

2.7. Challenges of E-Learning

Generally speaking, organisations make use of both Local Area Networks (LANs) and Wide Area Networks (WANs) for their day-to-day operations. The use of LANs is mostly visible in e-mail, Internet access, learning materials/resources and lecture handouts/materials, with some video-conferencing. Obviously, with these uses there is an issue of secured platforms and applications. Virtually all institutions make use of systems that track learner online activities. This may serve as a tool for securing networks but learner privacy is not provided. Most system development created to manage on-line learning is poor in this respect and thereby gives way for intruders and hackers. Some of the likely security threats in E-Learning are discussed in detail in Chapter three.

2.7.1. Inefficient Online Learner Support

How much support can be offered online? Not enough to meet the needs of learners whose learning style falls under category of hands-on, physical or face-to-face requirement. All individuals are different and so have different learning needs and styles (Van Doorn and Van Doorn, 2014). Generally, institutions are obliged to meet learner's needs through learner support. E-Learning developments are still on the way to developing E-Learning structures to meet all needs of learners as they arise.

2.7.2. Connectivity / Access Issues

The connectivity and access issues are of major concern as everyone wants to do something at any point in time. It is likely that networks may have to face dealing with traffic sometimes resulting in slow processes and operations. There are issues learners face in connectivity and bandwidth which will lead to problems in downloading of engaging content which will make the learning slower. This leads to frustration among the learners and affects the ease in the training and learning process (Agrawal, 2015).

2.7.3. Economic Factors – Affordability

At the moment most web-based course tuitions payments are made online using credit cards, direct debits, or even by authorisation of regular payment from credit cards. This works for some spending, but unless an individual has a merchant account the average person cannot accept income to their credit card. It is also important to bear in mind that not all countries are technologically buoyant.

2.7.4. Untrustworthy Learners

Certain learners may be reluctant to take part in electronic assessment, which is difficult for the tutor to ascertain trustworthy and untrustworthy online learners. Hence, the issue of cheating in assessments and tasks comes up. Some learners may not truly be involved in taking part in the learning process (course content), since by so doing they would be capable of having someone performing all their academic work for them- since they work in privacy in their homes or work place. However, this uncultured and deceitful attitude towards abusing the E-Learning system will result in such learners gaining certifications unworthily without putting genuine effort in courses. Actually, taking care of tuition payments tends to be the only effort made by such learners. E-Learning thus requires a lot of self-discipline and ethics on the part of the learner.

2.7.5. Technological Issues

Technology serves the driving force for E-Learning. Online learners need access to the right hardware and software apparatus, compatibility and sufficient bandwidth to achieve the best in their courses and training– as that should be the aim of every learner. Childs (2000) and Rana et al. (2014) also point that the frustrations and demotivational aspects of E-Learning is caused by technological limitations. The question now is: is lifelong learning over the Internet a reality? Technology has been known to be untrustworthy since its existence. Machines and systems will definitely go faulty at some point and so is regarded as an expected issue.

2.8.6. E-Learning Vulnerabilities

It is not a secret that E-Learning depends on the Internet. Nowadays, there are many illegal activities and security threats that take place on the Internet. The E-Learning system is constantly exposed to security threats, risks and attacks.

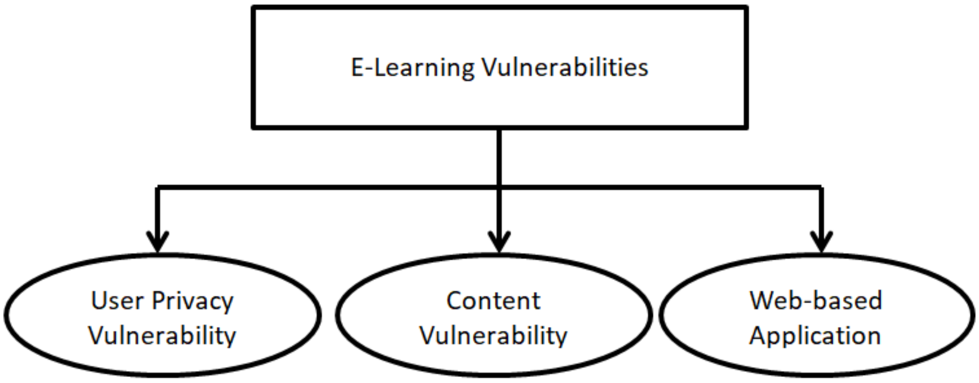


Figure 5. E-Learning Vulnerabilities

The following E-Learning vulnerabilities are caused by web attacks (see Figure 5) and will now be described in more details:

- User Privacy Vulnerability
  Privacy requirements are very important within E-Learning. In order to provide users with a personalised service, a user is often required to give personal information such as his/her name, job title, company, physical mailing address, e-mail address, telephone and fax numbers, and, if applicable, financial information such as a credit

card information. A learner has a right to keep his/her information private. According to Aïmeur et al. (2008), the reasons can be grouped under two categories:

- ✓ Competitive: when a prominent learner (e.g. a politician) is taking a course to increase his/her knowledge, which will give the learner an advantage over his/her opponents, he/she requires privacy and has the right to keep his/her results private from public knowledge and scrutiny.
- ✓ Personal: when a learner would like to protect himself from a biased tutor. Another reason a learner would prefer to keep his privacy is the increased pressure and stress due to performance anxiety.

It is very important to ensure a secure environment for data storage. There are cases in which data that is maliciously modified (by e.g. data tampering, data fraud and unauthorized data gathering) can produce serious and long-term consequences.

Personal information is very sensitive and its unauthorised disclosure even without modification or exploitation, e.g. identity theft, can lead to a negative impact on the institution's reputation. User tracking and logging all user requests can be exploited to extract patterns for identifying physical users behind recorded activities. Therefore, personal data essentially need to be considered as an asset within the E-Learning system.

- Content Vulnerability

  One of the most important issues in E-Learning system is content integrity. Unfortunately, many E-Learning systems do not provide content integrity protection. While using E-Learning system, users share files which is the primary means of downloading copyrighted digital properties. As a result, a legitimate user of E-Learning can easily violate digital property right of others by posting or disseminating the E-Learning content, such as lectures slides, tutorial video and software without authorisation. Graf (2002) suggested an approach to protect intellectual property by extending the control of the copyright holder to the entire lifetime of digital data. He suggested a method called CIPRESS which controls the access to the material. Graf describes mechanisms for copyright protection and tracing approaches using digital watermarking in such a way that information about a user who requested some data will be stored within the multimedia assets, and, therefore, any illegal copy can be traced back to that user who most probably distributed the content.

- Web-based Application Vulnerability

  According to Reavis (2012), web-based applications are vulnerable to many attacks due to: 1) not running the latest updates and patches on a web server, web applications, and developer machines; 2) new vulnerabilities due to increase interactivity on websites; 3) issues associated with the actual coding (with newer trends like cloud, social networking, and mobile, web designers may inadvertently introduce new vulnerabilities that need to be identified).

2.9. E-Learning and Security Requirements

Nowadays we often hear the question asked, “What is Security?”. Depending on the context, security might even mean different things to the same person (Viega et al., 2001). According to Encyclopaedia Britannica (2015), most security and protection systems emphasize certain hazards more than others. In a retail store, for example, the principal security concerns are shoplifting and employee dishonesty (e.g., pilferage, embezzlement, and fraud). Marshall E-Learning Consultancy (2018) stated that in 2015 the average cost of online Information Security breaches was £1.5 million. Users' security awareness is critical in E-Learning system where security policies and procedures require constant update (Security Industry Authority, 2016).

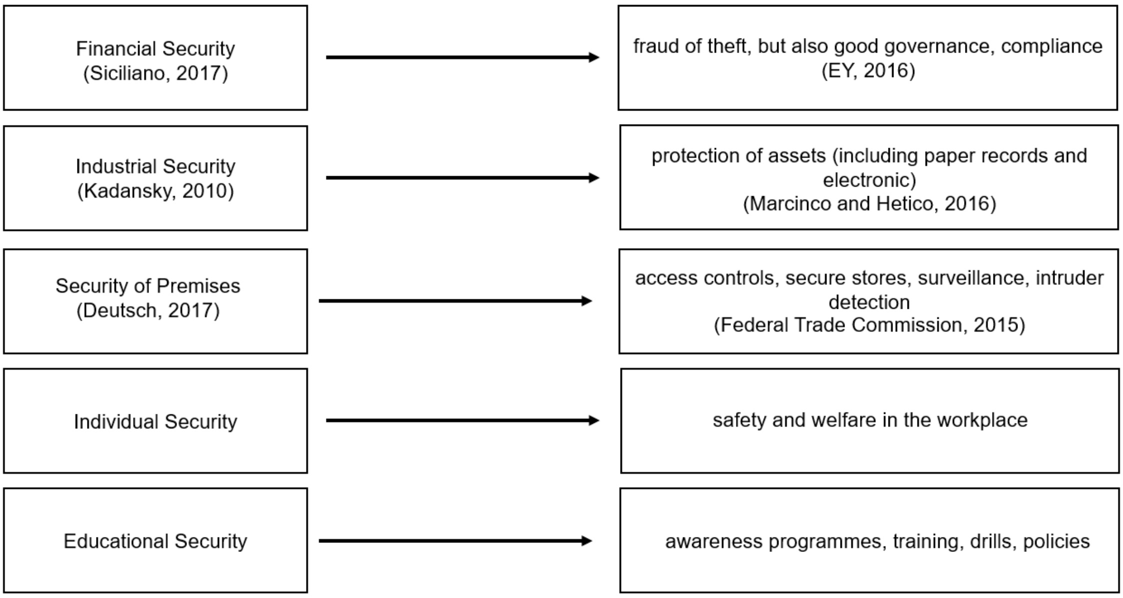

Financial Security (Siciliano, 2017)
fraud of theft, but also good governance, compliance (EY, 2016)
Industrial Security (Kadansky, 2010)
protection of assets (including paper records and electronic) (Marcinco and Hetico, 2016)
Security of Premises (Deutsch, 2017)
access controls, secure stores, surveillance, intruder detection (Federal Trade Commission, 2015)
Individual Security
safety and welfare in the workplace
Educational Security
awareness programmes, training, drills, policies

Figure 6. List of Some Security Concerns in Everyday Life

A typical set of categories to be protected includes the personal safety of people in the organization, such as employees, customers, or residents; tangible property, such as the plant, equipment, finished products, cash, and securities; and intangible property, such as highly classified national-security information or "proprietary" information (e.g., trade secrets) of private organizations. Without doubt, security means different things to different people (see Figure 6).

Meeting the security requirements in an E-Learning system is an extremely complex issue, because it is necessary to protect the content, services and the personal data not only for the external users, but also for the internal users, including system administrators. Despite all technical security aspects, users within E-Learning system are the weakest link of the security concept. In relation to security in E-Learning, security policies can be very helpful for users and can direct them on how to act correctly within an E-Learning system. Research in the E-Learning domain has mainly focused on providing and delivering content and infrastructure. Security issues are usually not taken as a central concern in most implementations either because systems are usually deployed in controlled environments, or because they take the one-to-one tutoring approach, not requiring strict security measures.

Clinch (2009) classifies core and secondary security concepts (see Figure 7). The core Security concepts comprise of confidentiality, integrity and availability.

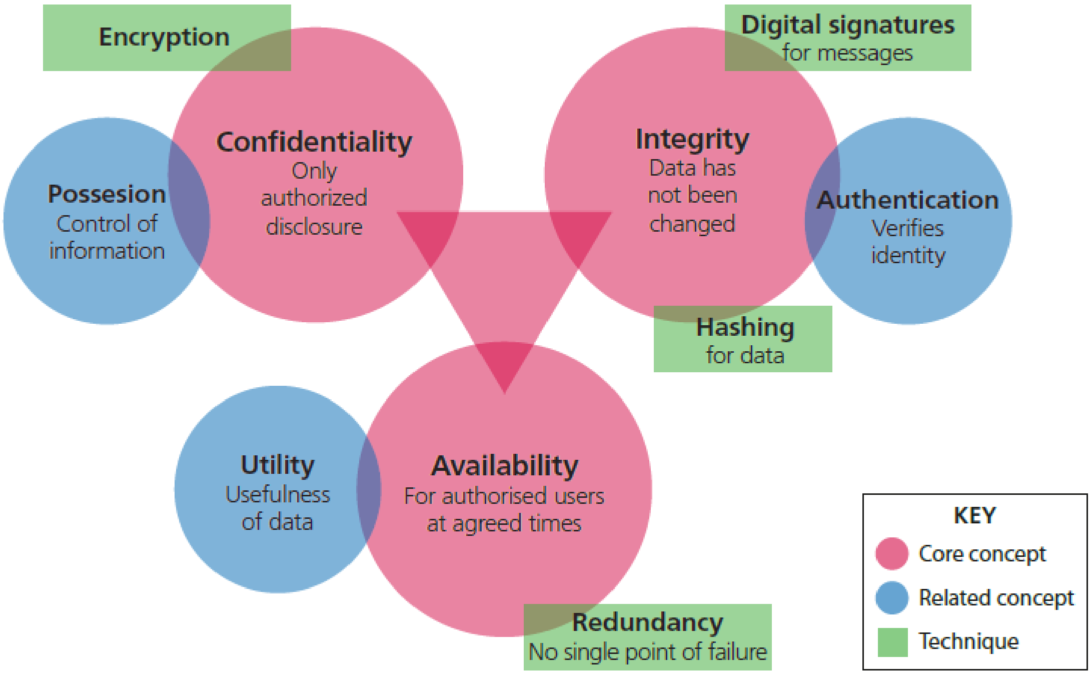


Figure 7. Core and Secondary Information Security Concepts (Clinch, 2009)

Kritzinger and von Solms (2006) identify six information security measures to ensure a secure E-Learning system:

2.9.1. Identification and Authentication

The first part of this service is to determine whether or not a person, who is trying to gain access to a system, has it granted. This process is known as identification and a user ID is usually entered to gain access to a system. After identifying a user, the system must ensure that a user is the one who he or she claims to be. This process is called authentication. Levy (2011) discussed user authentication as an important issue to consider in E-Learning security. The work shows that with varying software and hardware requirements, policies and strategies should be put in place to ensure appropriate authentication of the learner. Authentication controls have three common factors that challenge what: a user knows (a password), a user has (a token), or a user is (a biometric) (Furnell, 2007). Authentication can be done if a user utilizes something he/she knows (e.g. password), something he/she has (e.g. access card) or something he/she is (e.g. fingerprints). The examples of the information security countermeasures for identification and authentication are passwords and login IDs. Passwords can be easily distributed so this authentication method is often considered inadequate to protect critical E-Learning activities from impersonation fraud (Apampa et al., 2010). Biometric authentication system has been proposed to be the next option for future e-learning users (Wang et al., 2013). Biometrics is defined as the identification of an individual based upon the uniqueness of physiological and behavioral characteristics, which is a stronger authentication than simply using passwords (Gao, 2012). Biometric authentication may only deter impersonation because an imposter can take over the activity once the biometric is matched (Apampa at el., 2010; Song et al., 2013a). Song et al. (2013b) proposed another method that uses brain wave and eye movement to authenticate users of online learning systems.

2.9.2. Authorisation

Sagar and Waghmare (2016) stated that authentication refers to a mechanism in which the authorisations provided are compared to those on file in a database of authorized users' information within an authentication server. This service ensures that properly identified and authenticated users can only have access to those electronic resources for which they are authorised. One of the examples of the information security countermeasures for authorisation is Access Control.

2.9.3. Confidentiality

Confidentiality refers to the assurance that information and data are kept secret and private and are not disclosed to unauthorized persons, processes or devices. It is a requirement to keep sensitive information from being disclosed to unauthorised users (Jung et al., 2001). In an E-Learning perspective, students need the assurance that their assignments they submit online are kept private and only disclosed to the intended examiner. One of the examples for the information security countermeasure for confidentiality is encryption. Security is an important factor in e-learning system. The goal of security for e-learning is to maintain the confidentiality of data or information, integrity of information and availability of e-learning resources at a certain level while keeping their usability acceptable for learners (Adetoba et al., 2016).

2.9.4. Integrity

Integrity depends on access controls; therefore, it is important to positively and uniquely identify all persons who attempt access. Integrity can be compromised by hackers, masqueraders, unauthorised user activity, unprotected downloaded files, LANs, and unauthorised programs (e.g., Trojan horses and viruses), simply because each of these threats can lead to unauthorised changes to data or programs (Adetoba et al., 2016). According to Bishop, *integrity* refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity ensures that all information stored in databases and /or transmitted over networks, can only be changed by properly authorized users (Bishop, 2004). The integrity of data depends not only on whether the data is 'correct', but whether it can be trusted and reliable. Integrity is an indication of information accuracy and reliability (Jung et al., 2001). One of the examples of countermeasures to ensure integrity is message authentication codes.

2.9.5. Non-repudiation / Non-denial

The non-repudiation is about obtaining a proof that the announced participant really performed a given transaction and that this proof can be verified even without the consent of the said submitter. In this respect, non-repudiation cannot be imposed by means of symmetric cryptography since verification can be done without the submitter's consent and thus it cannot use whatever credentials (e.g., secret keys, passwords etc) the submitter may own. Therefore, non-repudiation usually mandates the use of some sort of Public Key Infrastructure (PKI). After that, non-repudiation can be realized by the use of digital signatures that act much like a written signature. This situation also requires that all participants own a digital certificate which bounds their public key with their true identity (Kambourakis and Damopoulos, 2013). For instance, whenever student submit assignments, it must be possible to reliably trace the activity. An example of an information security measure for non-repudiation is that of digital signatures (see sub-section 6.1. Proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

2.9.6. Availability

Availability refers to the assurance that information and communication resources are readily accessible and reliable in a timely manner by authorised persons. In an E-Learning perspective, students need the assurance that they have reliable and timely access to the E-Learning system in order to submit their assignments on time. One of the examples of the Information security countermeasures for availability is backups. The availability of materials and information to be accessed at any point in time and at any location is crucial. Failing to fulfil this will have a huge impact on E-learning users and providers (Alwi and Fan, 2010). In E-Learning, availability is the assurance that the e-learning environment is accessible by authorised users, whenever it is needed.

The literature review shows that the proposed information security measures for E-Learning system by Kritzinger and von Solms (2006) are not used as best practice or benchmark. Undoubtedly, the implementation of E-Learning systems in higher education has enabled a dramatic change in teaching and learning practice. The success of E-Learning adoption across an organization depends on several factors, for example, the availability of technology, how students and instructors are supported in its use and the integration of technology within the student learning experience (Adelabu et al., 2014).

2.10. Working Groups on Security Management Standards

To develop an online E-Learning solution there are several factors and standards of distance learning in education to be considered, which will influence its survival and the growth in the future market. For different online learning vendors the main factors which are vital to sell the products in the markets are standardisation and compatibility. There is also a factor to check whether different E-Learning systems are compatible with one another or not. The following groups are seeking to develop the standards for the E-Learning standards:

- IEEE is an international organization that develops technical standards and recommendations for electrical, electronic, computer and communication systems. Within the IEEE, the Learning Technology Standards Committee (LTSC) provides specifications that address best practices, which can be tested for conformance. Basically, they wrote the standard on how to write standards. The most widely acknowledged IEEE LTSC specification is the Learning Object Metadata (LOM) specification, which defines element groups and elements that describe learning resources. The IEEE P1484 is the model which was proposed by IEEE LTSC (Muramatsu, 2008). It involves the specification of Public and Private Information (PAPI) which effectively describes all the variances that deal with the privacy and the security features using the learner's information. They may create, store, retrieve the users information by using specific entities. It categorizes the views related to security from the different stakeholders involved in the system, such as developer, regulator etc. It also chooses the different entities involved in the customer management like their contact information, preferences, performance, personal information and portfolios.

  As explained above it does not explain a specific structure or a model or a technology but it explains all the security issues implemented in order to provide privacy factor. Also, it does not provide any privacy or a security policy. It only explains that the administrators and the learners will act as the policy makers by applying the policy factor of privacy using certain security techniques and technologies. It uses a factor of logical division of learner information. Once the learner information gets stored on a server it will become de-identified, partitioned and compartmentalized which will cover most of the privacy and security factors related to the user.

- Aviation Industry CBT Committee (AICC) is an international group of technology-based training professionals that creates CBT-related guidelines for the aviation industry (Aviation Industry CBT Committee, 2008). AICC publishes a variety of recommendations, but its standards with the most impact on the E-Learning arena are its computer managed instruction (CMI) guidelines. The AICC focuses on practicality and provides recommendations on E-Learning platforms, peripherals, digital audio, and other implementation aspects (Yong, 2007).

- The IMS Global Consortium is a consortium of suppliers that focus on the development of specifications that focus on the use of metadata to address content packaging (Brandon, 2013). The specifications are used to define how an LMS communicates with back-end applications and content objects or libraries. Several of its standards are made available on its website at no fee. The IMS global learning consortium (IMS GLC) is an organization intended to develop open specifications for distributed learning (Sammour, 2013). This is involved in addressing the key challenges and problems in distributed learning environments with a series of reference specifications which include Meta-data specifications, Enterprise specification, content and packaging specification, question and test specification, simple sequencing specification, and learner's Information Package specification (Şerb et al., 2013). Among all the specifications mentioned above IMS Learners Information package deals with the interoperability of the Learner's Information systems with other systems which are supported by the Internet learning environment (Botsios and Georgiou, 2010).

  It employs different ways to capture learners' information which includes their education record, training log, professional development record, and life-long learning period, community service record (e.g. work and training experience). With the help of the learner's information the system can be made to respond to specific needs of the user or learner (Fishman and Sledge, 2014). By employing the learners' information server the learning system can be efficiently utilised by the user. The certain mechanisms in the IMS (Learner Information Package) LIP specification are enabled in order to maintain privacy and security for the learners. A learner information server is responsible for sending and receiving learner's data to other information systems or other servers. The server is administered or monitored by a special authorized person (Şerb et al., 2013). All the packages that are needed for importing or exporting the data from the Learner information server are provided below. Data Privacy and integrity are considered to be the most vital requirements for the IMS LIP specification. Nevertheless, the IMS LIP specification does not avail the facility of having a look at the details of Implementation mechanisms or architectures that are employed for providing security and integrity to the Learners Information. The IMS LIP final specification V1.0 is not providing any following structures for enabling any suitable architecture for learner privacy protection (Kumar and Chelikani, 2011).

- The Alliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE) focuses mainly on meta-data specification of electronic learning materials with the goal of sharing and reusing these materials (El-Khatib et al., 2003).

- Advanced Distributed Learning (ADL) is a U.S. government-sponsored organization that researches and develop specifications to encourage the adoption and advancement of E-Learning (Bao and Castresana, 2012).

- ISO/IEC 27001 is the best-known standard within the ISO/IEC 27000 compliance. It establishes the standard requirements for implementing, maintaining and continually improving an information security management system for the purpose of the organizational business operation. The ISO/IEC 27001 is also used for assessment of information security risks based on the needs of the organisation. The requirements of ISO/IEC 27001 are generic and are intended to be applicable to all organizations, regardless of type, size or nature (ISO/IEC 27001, 2013).

Generally speaking, E-Learning is mostly associated with activities involving computers and interactive networks. The computer does not need to be the central element of the activity or provide learning content. However, the computer and the network must hold a significant involvement in the learning activity (Tsai and Machado, 2002; Hussein, H.A, 2015). Related terms to E-Learning include: Distance Education, Online Education, Distributed Learning, Internet Education, Computer-based Training, Computer-Mediated Communication, Computer-Assisted Instruction, Virtual Learning Environment (VLE), Cyber-Learning, Asynchronous Learning, Mobile Learning (M-Learning) and Multi-modal Instruction (Usu, 2003; Pop, 2016). The meanings of these terms are starting to converge. Where there is a difference in usage is explained by place (same place, any place, on-campus, off-campus); time (same time -- synchronous or not at the same time -- asynchronous); interaction (learner to computer; learner to instructor; learner to other learners); use of the computer (presentation, interactive, collaborative, generative); type of technology (text, audio, video, multimedia); and absence or presence of face-to-face interaction (Odhiambo and Acosta, 2009; The University of British Columbia, 2010).

2.11. Security Threats in E-Learning

Security is closely related to the actual threat. According to Recommendation X.800 of the International Telecommunication Union (ITU) (1991) "...security features usually increase the cost of a system and may make it harder to use. Before designing a secure system, therefore, one should identify the specific threats against which protection is required".

E-Learning is largely dependent on the Internet. Without doubt, there are many security threats and attacks that take place on the Internet. The E-Learning systems are vulnerable to several types of web attacks. Attackers can use phishing and spyware attacks to steal user credentials. The attackers can then easily gain access to the server using the stolen user credential. Nowadays, the course materials in the server are protected using watermarks. However, the protection can be broken by using several attacks, e.g.: removal attack, geometric attack, cryptographic attack and protocol attack (Voloshynovskiy et al., 2001). The attackers can also implement social intersection attack to identify the source of shared sensitive data with very high accuracy. This attack effectively works in collaborative E-Learning system and nearly impossible to be detected. Furthermore, the attackers can consider the following attacks by taking into consideration web vulnerabilities: Cross Site Scripting or XSS (Shar and Tan, 2012; Van Gundy and Chen, 2012), Cross Site Request Forgery (CSRF) (Siddiqui and Verma, 2011; Sun et al., 2012), SQL injection (Bashah Mat Ali et al., 2011; Natarajan and Subramani, 2012) and password cracking (Jing et al., 2011; Kelley et al., 2012). Barik and Karforma (2012) discussed various security risks or threats in E-Learning. Some of which includes confidentiality violation, integrity violation, denial of service, etc. and providing remedies to minimise all these risks. Some of the attacks are described in the sub-sections below:

2.11.1. Cross Site Scripting (or XSS)

Cross Site Scripting (or XSS) is one of the most common application-layer web attacks. It is one of the most common application level attacks that hackers use to sneak into web applications today. Cross site scripting is an attack on the privacy of clients of a particular web site which can lead to a total breach of security when customer details are stolen or manipulated (Klein, 2002). XSS commonly targets scripts embedded in a page which are executed on the client-side (in the user’s web browser) rather than on the server-side. XSS in itself is a threat which is brought about by the Internet security weaknesses of client-side scripting languages, with HTML and JavaScript as the prime culprits for this exploit (Shar and Tan, 2012; The Phantoms, 2017). The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the malicious user. An XSS attack can be used to achieve the following malicious results:

- accessing sensitive information;
- identity theft;
- altering browser functionality;
- web application defacement;
- denial of service attacks.

The XSS attacks can be categorized as Persistent, Reflective and DOM-based (Uto and Melo, 2009). In the first case, the malicious code is permanently stored on server resources. Persistent is the most dangerous type of XSS (Xu et al., 2006). In the second case, the code runs in the client browser without being stored on the server. This attack is usually made possible through links to malicious code injection. According to the OWASP (2011) (Open Web Application Security Project), this is the most frequent type of XSS attack. Finally, instead of using malicious code embedded into the page that is returned to the client browser, the DOM-based XSS enables dynamic scripts on components of the document, modifying the DOM environment (Document Object Model).

2.11.2. Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) is an attack that tricks the victim into loading a page that contains a malicious request. It is malicious in the sense that it inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf, like change the victim's e-mail address, home address, or password, or purchase something. A successful CSRF attack can be devastating for both the business and user. It can result in damaged client relationships, unauthorized fund transfers, changed passwords and data theft - including stolen session cookies (Imperva, 2018). For most sites, browsers will automatically include with such requests any credentials associated with the site, such as the user's session cookie, basic auth credentials, IP address, Windows domain credentials, etc. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish this from a legitimate user request. In this way, the attacker can make the victim perform actions that they did not intend to, such as logout, purchase item, change account information, retrieve account information, or any other function provided by the vulnerable website.

2.11.3. Structured Query Language (SQL) injection

The Structured Query Language (SQL) injection is a relatively simple type of attack. Using this method, a hacker can pass string input to an application with the hope of gaining unauthorized access to a database. Hackers enter SQL queries or characters into the web application to execute an unexpected action that can then act in a malicious way. Such queries can result in access to unauthorized data, bypassing of authentication or the shutdown of a database even if the database resides on the web server or on a separate server (Ciobanu and Ciobanu, 2012). SQL injection vulnerabilities are:

- check the user's input for dangerous characters like single-quotes;
- using prepared statements, which tell the database exactly what to expect before any user-provided data is passed to it;
- encrypt sensitive data;
- ensure that error messages give nothing away about the internal architecture of the application or the database.

The SQL injection can be applied also for URLs, which can be modified by an attacker in order to access important information. By leveraging an SQL Injection vulnerability, given the right circumstances, an attacker can use it to bypass a web application’s authentication and authorization mechanisms and retrieve the contents of an entire database. SQL Injection can also be used to add, modify and delete records in a database, affecting data integrity (Acunetix, 2018).

2.11.4. Stack-smashing attacks

Stack-smashing attacks target a specific programming fault: careless use of data buffers allocated on the program's run-time stack, namely local variables and function arguments. Stack-smashing attacks are a serious problem. The idea of stack-smashing attacks is when some attack codes are inserted (e.g., code that invokes a shell) somewhere and they overwrite the stack in such a way that control gets passed to the attack code (Ciobanu and

Ciobanu, 2012). In 2016, Cisco published technical details of the vulnerability and demonstrated an attack against the Bitcoin-qt Wallet, the default Bitcoin client. An attacker would need to set up a phony UPnP server on the local network that would serve up an XML file with “overly long element names,” Cisco said. Cisco’s exploit bypasses a mitigation in place called Stack Smashing Protection (SSP), which protects vulnerable buffers in a stack with a stack cookie, or canary. The cookie is a fixture in UNIX and Linux builds; Microsoft also deploys a similar mitigation. The Cisco attack bypasses the stack cookie on Linux systems (Mimoso, 2016).

2.11.5. Session hijacking

Session hijacking is the exploitation of a valid computer session, sometimes also called a session key, to gain unauthorized access to information or services in a computer system. According to Miletic (2011), this means stealing the magic logon hash from the session cookie. The attack is possible when session id is weakly encrypted, too short or assigned sequentially. The biggest advantage of a session hijacking is that the malicious attacker can enter the server and access its information without having to hack a registered account. In addition, he can also make modifications on the server that to help him hack it in the future, or to simplify a data stealing operation (Heimdal Security, 2017). Sessions that do not expire on the HTTP server can allow an attacker unlimited time to guess or brute-force a valid authenticated session id and eventually gain access to that user's web accounts (Ciobanu and Ciobanu, 2012). To prevent issues regarding the session security, the following best practices should be followed:

- session ID should be adequately long and unpredictable;
- check if the session ID is valid;
- check if the session ID has been generated by the application (was not manually introduced by the user);
- regenerate session ID after a period of time or when the user privilege level has changed;
- use only cookies to propagate session ID;
- avoid “remember me” option;
- expire session on security error;
- expire session after a period of inactivity;
- remove session cookie when a session is destroyed.

2.11.6. Removal Attacks

Removal attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm, e.g., without the key used for watermark embedding. Sophisticated removal attacks try to optimise operations like denoising or quantization to impair the embedded watermark as much as possible while keeping the quality of the attacked document high enough (Voloshynovskiy et al., 2001; Yasin et al., 2015). Recent results show that a small number of different copies, e.g., about 10, in the hand of one attacker can lead to successful watermark removal (Voloshynovskiy et al., 2001). The removal attacks include denoising, quantization (e.g., for compression), remodulation, and collusion attacks. Not all of these methods always come close to their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly (Sunesh, 2011).

2.11.7. Geometric Attacks

The geometric attacks are one of the most important issues in digital watermarking (Li, 2010). Many researchers have proved that even very small geometric distortions can prevent the detection of a watermark (O'Ruanaidh et al., 1998; Lin et al., 2001; Xiang et al. 2008). Digital watermarking has been proposed as a solution to the problem of copyright protection of multimedia documents in networked environments (Liu and Tan, 2002). The geometric attacks mainly introduce synchronization errors between the encoder and decoder. The watermark is still present, but the detector is no longer able to extract it (Veerappan and Pitchammal, 2012). Geometric attacks are classified basically into two types as global geometric and local geometric attacks. Global geometric attacks affect all the pixels of an image in similar manner. The examples include rotation, scaling, translation etc. Local geometric attacks affect different portions of an image in different ways. These attacks include cropping, row-column blanking, warping etc. Rotation, translation and scaling attacks are examples of affine transform (Jabade and Gengaje, 2016).

2.11.8. Cryptographic Attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks (Voloshynovskiy et al., 2001). The examples of cryptographic attacks are as follows:

- The brute-force search for the embedded secret information;
- Oracle attack, which can be used to create a non-watermarked signal when a watermark detector device is available.

Hacker Bulletin (2016) identified the following types of cryptographic attacks:

- Replay Attack (this attack is used against cryptographic algorithms that do not incorporate temporal protections. In this attack, the malicious individual intercepts an encrypted message between two parties (often a request for authentication) and then later "replays" the captured message to open a new session. This attack can be defeated by incorporating a time stamp and expiration period into each message).
- Man in the Middle Attack (in the man-in-the-middle attack, a malicious individual sits between two communicating parties and intercepts all communications (including the setup of the cryptographic session). The attacker responds to the originator's initialisation requests and sets up a secure session with the originator. The attacker then establishes a second secure session with the intended recipient using a different key and posing as the originator. The attacker can then "sit in the middle" of the communication and read all traffic as it passes).
- Implementation Attack (this is a type of attack that exploits weaknesses in the implementation of a cryptography system. It focuses on exploiting the software code, not just errors and flaws but the logic implementation to work the encryption system.
- Statistical Attack (it exploits statistical weaknesses in a cryptosystem, such as floating-point errors and inability to produce truly random numbers. Statistical attacks attempt to find a vulnerability in the hardware or operating system hosting the cryptography application).
- Frequency Analysis and the Ciphertext Only Attack (In many cases, the only information you have at your disposal is the encrypted ciphertext message, a scenario known as the ciphertext only attack. In this case, one technique that proves helpful against simple ciphers is frequency analysis—counting the number of times each letter appears in the ciphertext. Using your knowledge that the letters E, T, O, A, I, and N are the most common in the English language, you can then test several hypotheses: -If these letters are also the most common in the ciphertext, the cipher was likely a transposition cipher, which rearranged the characters of the plain text without altering them. -If other letters are the most common in the ciphertext, the cipher is probably some form of substitution cipher that replaced the plaintext

characters. This is a simple overview of frequency analysis, and many sophisticated variations on this technique can be used against polyalphabetic ciphers and other sophisticated cryptosystems).

- Known Plaintext (in the known plaintext attack, the attacker has a copy of the encrypted message along with the plaintext message used to generate the ciphertext. This knowledge greatly assists the attacker in breaking weaker codes).

2.11.9. Protocol Attacks

Protocol attacks aim at attacking the entire concept of the watermarking application (Voloshynovskiy et al., 2001). The main protocol attacks are described below:

- One type of protocol attack is based on the concept of invertible watermarks (Craver et al., 1998; Varshney, 2017). The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create ambiguity with respect to the true ownership of the data. It has been shown that for copyright protection applications, watermarks need to be non-invertible. The requirement of non-invertibility of the watermarking technology implies that it should not be possible to extract a watermark from a non-watermarked document. A solution to this problem might be to make watermarks signal-dependent by using one-way functions (Voloshynovskiy et al., 2001; Sherekar, 2011).
- Another protocol attack is the copy attack. In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data (Kutter et al., 2000). The estimated watermark is adapted to the local features of the target data to satisfy its imperceptibility. The copy attack is applicable when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor the knowledge of the watermarking key (Voloshynovskiy et al., 2001).

2.12. Copyright

Copyright is an exclusive right given to the primary author or creator of a work. According to the Copyright, Designs and Patents Act 1988 photocopying, scanning or copying a work using digital technology for education is prohibited. The Berne Convention defines copyrightable subject matter broadly to include every production in the literary, scientific and artist domains; whatever may be the mode of form of expression. Updating the Berne subject matter, the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property, commonly known as the TRIPS Agreement, expressly includes computer programs and compilations of data (Renner, 2016). However, the technology that can be used to make copies is not specified in the Act. The only reference to how copies are delivered came in 2003 when the UK law was amended by “The Copyright and Related Rights Regulations (Statutory Instrument No. 2498)” (oPSI, 2003) which:

- redefined broadcasts to specifically exclude Internet transmission (or podcasts);
- gave copyright holders the exclusive right to ‘communicate a work to the public’;
- defined this right as making the material available by ‘electronic transmission’, that is, via the Internet and/or broadcasting the work.

Furthermore, Miller et al. (1994) discussed the need to incorporate computer software ethics in the curriculum of each and every course about or utilizing computers. However, Roberts et al. (1998) suggest that many copyright holders consider new technology to be a threat to their livelihoods, as they are the ultimate copying machine for both students and staff. Malouff et al. (1996) argue that academic dishonesty, plagiarism, or cheating is a major problem in the evaluative educational system. Academic dishonesty is more detrimental to the educational community than stakeholders realize because it affects faculty, students, and administration (Boehm, et al., 2009; Fontana, 2009; Lipka, 2009; Wilkerson, 2009).

Maintaining intellectual property and obtaining revenue and preventing financial loss are important considerations for E-Learning content developers and providers, resulting in considerable research on the subject. As the Internet has public access, Austerberry (2002) defines the two main goals of digital rights management as maintaining confidentiality and providing restricted access to entertainment. Lin et al. (2001) describe the main issues of copyright control as concerning conditional access, authentication, copy control/protection and content tracking.

In the case of streaming media, the bit stream needs to be protected from unauthorised access, which might result in tampering (Rees, 1994), copying and supply that would provide gain or a challenge for pirates and hackers. Conditional access is concerned with providing a licence (often subject to a fee), which allows the user to access the material, in some cases a restricted number of times. This may be enforced by the use of cryptography, so that a decryption key is necessary for the user to access the content. Keys can be either symmetric (shared secret) or asymmetric (public/private key) and can be delivered in a variety of ways.

In addition to providing authentication (verification of identity) of both the source and receiver, and authorization certificates cryptography can be employed to encrypt content (this is usually the first line of defence). For streaming applications, encryption must take place at the packet level to enable the viewer to view the content in real time. However, often more than one system is required if more than one architecture is provided. Encryption of streaming media can take place prior to storage or on the fly (Editvu-Security (2002), Austerberry (2002). Wolfgang et al. (1999) believe that encrypted digital content is of limited use because the media becomes unviewable. The same authors cite time stamping, where the owner of the media file can be ascertained from the earliest time stamp, as "critical to the success of any multimedia security system". The copy control is involved with the protection against unauthorised copying of material and often employs the use of watermarking technology. Digital watermarking technology has many applications in protection, certification, distribution, anti-counterfeit of the digital media and label of the user information (Singh and Chadha, 2013). Overtly visible watermarks tend to be employed for preview copies, while invisible digital watermarks, also known as perceptual watermarks, are used for high quality content, and can be tracked using Web spiders. Digital watermarks should be robust against attack and data conversion manipulation, imperceptible and informative, while their embedding and retrieval should be fairly straightforward, including in real-time situations. Watermarking of digital video is challenging as the stored transmitted content is often compressed, the watermarks can be damaged as a result of errors in the transmission network and because attackers could deduce a watermark from a comparison of different frames.

Audio content can also be watermarked, which is particularly challenging as a result of the sensitivity of the human audible system and the lower sampling rates of data in which to embed information. Hartung and Kutter (1999) cite several techniques which have been used successfully to embed watermarks in audio content. To discuss possible ideas and solutions for security and privacy enhancement of Copyright in E-Learning, it is necessary to identify the following security and privacy mechanisms:

- To protect the author's E-Learning content from copyright infringements
- To protect from unauthorized use of digital content. Weippl (2005) identifies two different groups of people who might use digital content in ways not intended by the author:

(i) People with legitimate access: Users who have legitimate access to the content may copy or modify it without permission and hand it to friends or make it available on the Internet. Addressing this threat is very difficult. The music industry has been struggling for years to fight the spread of MP3 files. One approach that currently still does not work well is systems that enforce digital rights management. Another option is to distribute only the content in formats that make illegal reuse more difficult: for instance, PDF files cannot be modified easily compared to PowerPoint.

(ii) People who access the content without authorisation: It is much easier to prevent people without authorization from accessing content. Almost all E-Learning systems provide mechanisms of access control that limit access to content. Nonetheless, even if the E-Learning system prevents unauthorised use, underlying layers such as the operating system or the database system on which the E-Learning system is installed may allow unauthorised users to gain access. It is therefore necessary to ensure that access control is enforced on all layers. This also includes physical access to the servers (Weippl, 2005).

Copyright has a number of justifications – that it is right and just to reward and recognise creative skill and effort, it provides an incentive to creators, and law-makers recognise these. Digitisation continues to pose fundamental challenges to copyright which have only been partially addressed by the 2003 Regulations (Stokes, 2014). Some argue that content-filtering technology might ultimately be the least expensive way of enforcing copyright law. Installing content filters might incur a cost, but this cost is less than the cost of installing rights-management technology everywhere else, or of pursuing large numbers of individual infringers through the existing court system (Sheppard, 2014).

Acquiring and demonstrating the appropriate knowledge, skills and behaviours to enable the ethical creation and use of copyright material has been referred to as 'copyright literacy' (Morrison and Secker, 2015). A discussion paper by the UK Government's intellectual property adviser recommended that copyright education should be embedded in the school curriculum within a range of subject areas (Weatherley, 2014). In some universities an understanding of copyright is being taught to students as part of digital literacy or entrepreneurship programmes, so students understand how to respect others' intellectual property and protect their own. According to Secker and Morrison (2016), standalone copyright courses inevitably suffer from poor attendance, with many teaching staff citing lack of time and viewing copyright as a low priority for their professional development. Therefore, it is essential to develop a positive message about copyright literacy and to offer a range of tailored (and well publicized) courses and online support materials.

2.13. Access Control

Access control is the way in which an application grants access to its content and function to different users. Granting and revoking privileges is a typical way of providing access control. Privileges are described as what allows specific users to access the application to do only what they are allowed to do (Connolly and Begg, 2005). The access control is realized during the authentication time when the user is granted with all the necessary rights. In this way the user will perform in the system only his allowed operations (Costinela – Luminitaa, 2011). When authorisation of users of a software application is not done properly, this could lead to various security breaches. This design flaw allows users or systems to perform actions that they should not perform. The presence of security flaws is not difficult to discover and exploit. All it would take the attacker is to request for access to functions or content which normally he/she does not have any privilege to access. If he is granted access, he would have discovered a flaw in the access control that can be exploited and the consequence can be disastrous. In this case, the attacker would have access to unauthorized content that is not properly protected which he may be able to change or delete, execute arbitrary code or manipulate the application especially if he is granted an administrator (OWASP, 2010).

Rana (2011) stated that access controls are the collection of mechanisms that specify what users can do on the system, such as what resources they can access and what operations they can perform. In computing access control refers to security features that control which principals (persons, processes and machines) have access to which resources. To achieve this, various access control models such as Discretionary Access Control, Mandatory Access Control (Infosec Institute, 2018), Role-Based Access Control (Kamoun and Tazi, 2014), Team-based Access Control (Malik et al., 2017), Task-Based Access Control (Thomas and Sandhu, 1998; Wang and Jiang, 2015) and Attribute Based Access Control (Karp et al., 2009; Kerr and Alves-Foss, 2016) have been developed.

From these access control models and others, Role-Based Access Control has proved to be more popular and is considered as an efficient way of assigning access rights to users while at the same time ensuring data security. Despite its popularity, Role-Based Access Control is criticised for its difficulty in setting up an initial role structure and for its inflexibility in rapidly changing environments (Kuhn et al., 2010). To cater for dynamic environments like E-Learning, which involve processing, transmitting and storing sensitive information, Role-Based Access Control needs to be enhanced with dynamic contextual attributes such as the subject's current location, current date and time of the day.

Access Control has existed as a concept for as long as humans have had assets worth protecting (Sandhu and Samarati, 1994). The goal of an access control system is to allow only authorised users to access resources (Sandhu, 1998, NIST-IR-7298, 2006). Guards, gates, locks and PIN in ATM cards are examples of access controls which we use in our daily lives (Kamoun and Tazi, 2014). With the advancement in ICTs, currently access control is mostly associated with the ways in which users can access information and resources in a computer system. In this section, definition of access control is provided together with a discussion and analysis of its prominent models. Security is a major concern for E-Learning information systems that process, transmit and store sensitive E-Learning records, which hold personal data about individuals, and access control is at the heart of this concern (Rostad et al., 2006). While authorised E-Learning professionals need access to the right information at the right time to provide the best possible study materials, it is also important to ensure E-learners' privacy. According to NIST (NIST-IR-7298, 2006), access control is defined as the process of granting or denying specific requests:

- For obtaining and using information and information processing services and
- To enter specific physical facilities.

A fully integrated E-Learning system should provide different groups of users such as program directors, course authors, editors, course coordinators, tutors, students and administrators with access to different web documents and Web services. Therefore, the access control of such Web-based E-Learning systems has become an issue for both researchers and practitioners in E-Learning.

Many researchers have contributed to Access Control in E-Learning. Sanka et al. (2010) proposed access control model by means of capability lists, determining who uses what. They revised Diffie-Hellman exchange protocol to exchange keys between providers and consumers. But the cons are that the model fails to manage policy conflicts, not dynamic and could not be implemented in heterogeneous platforms. Huang and Nicol (2012) proposed TrBAC (Temporal Role-Based Access Control). This work uses assurance index for measuring trust level. The con is that focusing on trust alone is not adequate for making access decisions. Zhou et al. (2013) proposed a new access control model called Context Aware Access Control model which ensures privacy and data security. A work by Chang et al. (2014) suggests that traditional RBAC and extensions to it does not provide complete solution. RBAC lacks in considering security levels amongst objects. In addition, they do not signify a variety of dynamic relationship amongst objects. An ARBAC mechanism for Multi-tenancy Cloud Environment was proposed by Lo and Guo (2015). They combined attribute and role-based access control mechanisms for finding which tenant the user can access.

They also used simple matrix calculation to fine-tune the access decision. This reduces compile time of XACML and even if the access information leaks out, the attacker could not identify it easily. Unfortunately, ABAC is not yet standardized. Hasan et al. (2016) described the following use case paths to control access in E-Learning system:

- Attempt to spoof through a legitimate user identity.
- Attempt to gain access through of unauthorized means.

They further identified the following threats:

- Misuser is validated by the system as an authorized user.
- Attempt to gain access through of unauthorized means, for hacking information from the system even though possessing legitimate access to the system.

Without doubt, E-Learning platforms have drastically improved today. Users can easily access the learning application on their personal devices at any time without boundaries restrictions. Due to learners' demands for flexibility in choosing different computers to learn wherever they want, possibilities to restrict access to certain services depending on the used physical clients are limited. For this reason, in this research it will be more appropriate to introduce location mapping to identify the user's location before granting access to the system.

Based on the results outlined in Chapter 4, users and account management component should be securely implemented to control access and allow different authorisation methods to E-Learning applications resources, complemented with the possibility of gathering data from resource providers. The security attacks, whether intentionally targeted or not, can originate from internal and external threats depending on the degree of exposure of assets and how vulnerable the system is to attack. Access control relies on and coexists with other security services in a computer system (Oppliger et al., 2004).

The various access control models have been developed over the years: Discretionary Access Control, Mandatory Access Control (Infosec Institute, 2018), Role-Based Access Control (Kamoun and Tazi, 2014), Team-based Access Control (Malik et al., 2017), Task-Based Access Control (Thomas and Sandhu, 1998; Wang and Jiang, 2015) and Attribute ased Access Control (Karp et al., 2009; Kerr and Alves-Foss, 2016). The Role-Based Access Control has proved to be more popular and is considered as an efficient way of assigning access rights to users while at the same time ensuring data security. Despite its popularity, Role-Based Access Control is criticised for its difficulty in setting up an initial role structure and for its inflexibility in rapidly changing environment (Kuhn et al., 2010).

2.13.1. Discretionary Access Control (DAC)

The Discretionary Access Control (DAC) is a means of restricting access to objects based on the identity of subjects and/or groups to which they belong (Infosec Institute, 2018). The control is discretionary in the sense that DAC leaves certain amount of access control to the discretion of the object's owner or anyone else, who is authorised to control an object's access (Hu et al., 2006). With DAC, the user who created the object has all the permissions about it and also can delegate his/her permissions to others. The DAC policy tends to be very flexible and has been widely used in commercial and government sectors. Despite its wide use, we consider this model as inappropriate for the E-Learning sector as E-Learning professionals create E-Learners' records, but they are not considered as the data owners and delegation can result into the breach of E-learners' privacy.

2.13.2. Mandatory Access Control (MAC)

The DoD (1985) defines MAC as a means of restricting access to objects based on the sensitivity of information contained in the object and the information authorisation, i.e. clearance of subjects to access information of such sensitivity. With MAC, security policy is centrally controlled by a security administrator and hence users do not have an ability to override the policy. The MAC policy is widely applied in military information systems where the individual data owner cannot decide who has the Top Secret Clearance nor can the owner change the classification of the object from the example *Top Secret* to *Secret*.

In relation to its use in E-Learning sector, like DAC, MAC is also considered inappropriate. For the E-Learning system, in case of emergency, the E-Learning professional requires an ability to override security policies in order to provide learning materials to E-learners. As previously discussed, this is not possible in MAC as only the central authority is allowed to make changes and therefore MAC is considered inappropriate for the E-Learning system.

2.13.3. Role-Based Access Control (RBAC)

In many organisations, users do not own information which they created or are allowed access to (Sandhu, 2001; Dekker, 2009). For such organisations, corporation/agency is the actual "owner" of the system objects as well as programs that process it and control is essentially based on the user's functions rather than data ownership (Dekker, 2009). When using job functions that an individual user take as part of the organisation to control access, then the model being considered is RBAC (Sandhu, 1998).

In RBAC, permissions are associated with roles and users are assigned to appropriate roles (Ferraiolo et al., 2003). This assignment greatly simplifies security administration (Kamoun and Tazi, 2014). Consider for example, if within a module or department, an E-learner's module has been changed to a core module, then the E-learner can be assigned to a new module (new role), and removed from the old one, whereas, in the absence of RBAC, the E-learner's old permissions would have to be individually revoked and new permissions would have to be granted. RBAC is also considered useful as it supports review of permissions assigned to users (see Figure 8).

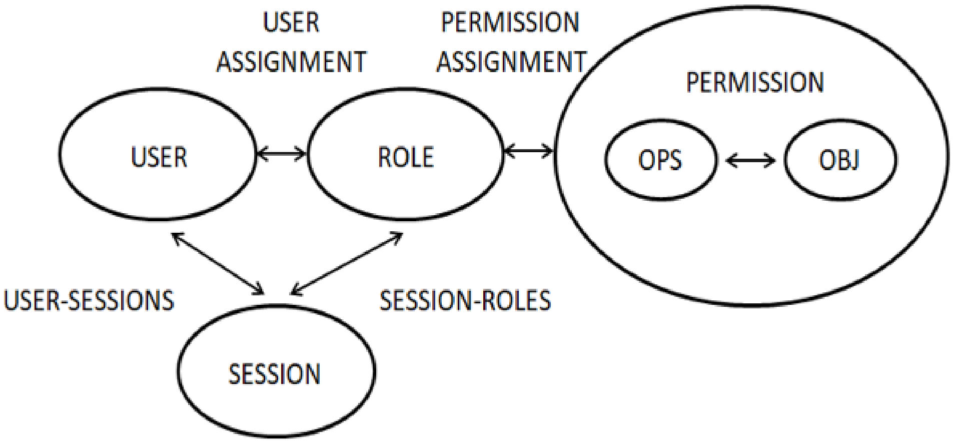


Figure 8. Role-Based Access Control (Sandhu et al., 1996)

Despite its various benefits, RBAC has frequently been criticised for its difficulty in setting up an initial role structure also known as role engineering and its inflexibility in rapidly changing environments (Kuhn et al, 2010). A pure RBAC solution may provide inadequate support for dynamic contextual attributes such as current location, current date and time of the day. Capturing context using RBAC would mean defining large set of roles for each possible contextual attribute. Moreover, to define fine-grained permissions would also create large sets of permissions and hence resulting into role explosion (Kuhn et al., 2010). To make RBAC simple and flexible for the dynamic environments like E-Learning, this widely used model need to be enhanced with contextual attributes.

2.13.4. Team-Based Access Control (TMAC)

The Team-Based Access Control (TMAC) is an approach of applying Role-Based Access

Control (RBAC) in collaborative environments where an activity is best accomplished through teams (Malik et al., 2017). Alotaiby and Chen (2004) describe a TMAC extension model, called TMAC04, built on RBAC which efficiently represents teamwork in the real world. The TMAC04 model allows certain users to join a team based on their existing roles in an organisation within limited context and new permission to perform the required work.

In relation to the identified need of contextual attributes which are considered important for providing fine-grained access control in a dynamic healthcare environment, TMAC does not bring anything new from RBAC's perspective.

Task-Based Access Control (TBAC): Contrary to other access control models where access rights are granted to subjects, with TBAC access rights are granted to tasks in steps related to the progress of the tasks (Thomas and Sandhu, 1998). Based on its provision of access rights to tasks, this model is considered as a dynamic access control technique (Moonian et al., 2008). TBAC is also considered to be suitable for automated processes where activities of the tasks cross computer boundaries. Despite being acknowledged as a dynamic access control technique, the use of tasks adopted by TBAC is regarded as a specific configuration of RBAC where context (tasks) can be viewed as constraints.

2.13.5. Other Access Control Models

Other access control models which are considered as the extensions of RBAC are Context-Based Access Control (CBAC) (Covington et al., 2001) and Proximity Based Access Control (PBAC) (Ardagna et al., 2006). CBAC is an extension of RBAC with the notion of environment roles in order to provide for security in context aware applications while PBAC is a specific case of CBAC.

The Attribute-Based Access Control (ABAC) is sometimes referred to as Policy Based Access Control (Blaze et al., 1999; Pimlott et al., 2006; Kerr and Alves-Foss, 2016) or Claims Based Access Control (Baier et al., 2010), is quite the opposite of RBAC. ABAC was introduced to address issues associated with the RBAC such as role explosion, which occurs when contextual attributes are captured and defined in RBAC and hence resulting in to thousands of roles associated with thousands of permissions. The ABAC's central idea is to use individual user's attributes to provide access decisions (Karp et al., 2009; Kuhn et al., 2010). As indicated in Figure 41, an ABAC policy specifies which claims need to be satisfied in order to grant access to the resource. Any user who can prove such a claim is granted access. For example, an ABAC policy contains the claim "above 18 years old", then any person who can prove this claim is granted access. Among the attributes associated with

ABAC include: the subject who is demanding access, the action which the subject want to perform, the resource being accessed and the environment or context in which access is requested. These four attributes are considered as general attributes which contain other attributes within (see Figure 9).

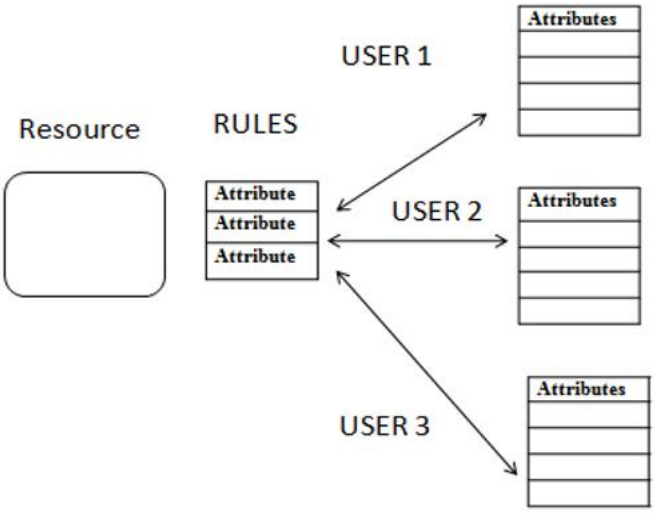


Figure 9. Attribute-Based Access Control (Karp et al., 2009)

Contrary to RBAC which is considered inappropriate for dynamic environments like E-Learning, as it does not support the use of context and capturing context may result in to role explosion, ABAC is considered to be flexible as it does not require separate roles for relevant sets of subject attributes and rules can be implemented quickly to cater for the changing needs (Karp et al., 2009).

In general, ABAC's approach made it easy to include context in the access control decisions. As a trade-off to its flexibility, this model suffers from complexity associated with the number of cases that need to be considered for the model as for *n* attributes or conditions using attributes, there are 2^n possible combinations. The model also requires an agreement on the meaning of attributes (Karp et al., 2009). For a dynamic E-Learning system, developing E-Learning information system which is purely RBAC, as most of the existing open source systems such as open source such as Care2X, OpenClinic, OpenEMR and FileMed and closed-source, is considered inappropriate. This is caused by the existence of various contextual attributes, which tends to affect security (Pfleeger and Cunningham, 2010) and hence make a contextual-aware authorisation to be of huge importance.

2.14. Characteristics of Access Control Models

Access control models bridge the gap in abstraction between policy and mechanism. Security models are formal presentations of the security policy enforced by the system, and are useful for proving theoretical limitations of a system (NIST, 2017).

As discussed in sub-section 5.1.2., Mandatory Access Control (MAC) takes a hierarchical approach to control access over resources. Under a MAC enforced environment, where single context is supported, access to all resource objects (such as data files) is controlled by settings defined by the system administrator, which means that in such environment access decisions are centrally controlled and it is not possible for users to change the access control of a resource.

Unlike the MAC where access to system resources is controlled by the system administrator, Discretionary Access Control (DAC) allows each user to control access to their own data. DAC provides a much more flexible environment than Mandatory Access Control but also increases the risk that data will be made accessible to users that should not necessarily be given access.

The Role Based Access Control (RBAC) is also known as Non-Discretionary Access Control, takes more of a real-world approach to structuring access control. Access under RBAC is based on a user’s job function within the organisation to which an information system belongs. The model uses a static security mechanism which is not highly flexible and provides no support for user mobility. Summary of the characteristics of each model discussed in this section is presented in Table 4.

Table 4. Characteristics of access control models

Models	No of Context	Dynamicity	Administration	Flexibility	User Mobility
DAC	Single	Static	Distributed	High	No
MAC	Single	Static	Centralised	Low	No
RBAC	Single	Static	Centralised	High	No
TBAC	Multiple	Dynamic	Distributed	High	No
TMAC	Multiple	Dynamic	Mixed	High	No
PBAC	Multiple	Dynamic	Centralised	Moderate	Yes
CBAC	Multiple	Dynamic	Distributed	High	Yes
ABAC	Multiple	Dynamic	Mixed	High	Yes

The CBAC, which is an extension of RBAC, is dynamic, distributed and provides enhanced user mobility (Zhang and Parashar, 2003), while with PBAC, which is a specific case o0f CBAC, there is support of multiple context and user mobility is supported using different proximity zones. The TBAC model extends the subject/object-based access control models by including domains that contain task-based contextual information. This model supports multiple context and hence supporting dynamicity and flexibility. The TMAC preserves the benefits offered by RBAC and also offers flexibility to activate permissions to individual users and to a specific object. ABAC, which uses user's attributes to control access, supports multiple context and hence considered appropriate for dynamic environments. The model also offers both centralised and distributed administration, together with user mobility.

2.15. Authentication

It is important to mention that Access Control works very closely with the authentication service. The responsibility of the authentication service is to correctly establish the identity of the user. If the authentication of the user has been successfully verified, Access Control can be enforced via a reference monitor. Passwords, the most common authentication methods, ask the user to provide a previously designated piece of knowledge (Sasse et al., 2001). According to Hawker (2000), methods of user identification can be classified into three main types, being based on:

- something you know (a password);
- something you possess (a token);
- one or more of your personal characteristics (biometrics).

Suo et al. (2005) stated that there are three different categories of authentication: knowledge-based, token-based, and biometric-based authentication.

2.16. Types of Authentication

The principles of authentication are widely acceptable in identifying users. The most commonly used authentication types are as follows:

2.16.1. Knowledge-Based Authentication (KBA)

The Knowledge-Based Authentication (KBA) is a security measure that is utilised in order to identify end users for accurate authorisation of online activities. The idea behind KBA is that by selecting questions that only the target individual would know the answers to, systems can verify whether a user is the legitimate owner of a password-protected area (IDology, 2014). The KBA refers to a method of authentication which requires a user to remember a sequence of secret numbers, answers to questions or graphical images as a password (see Figure 10), and in which the user is presented with a group of images and asked to recognise the image that he or she selected in the registration phase (Ma and Feng, 2011).

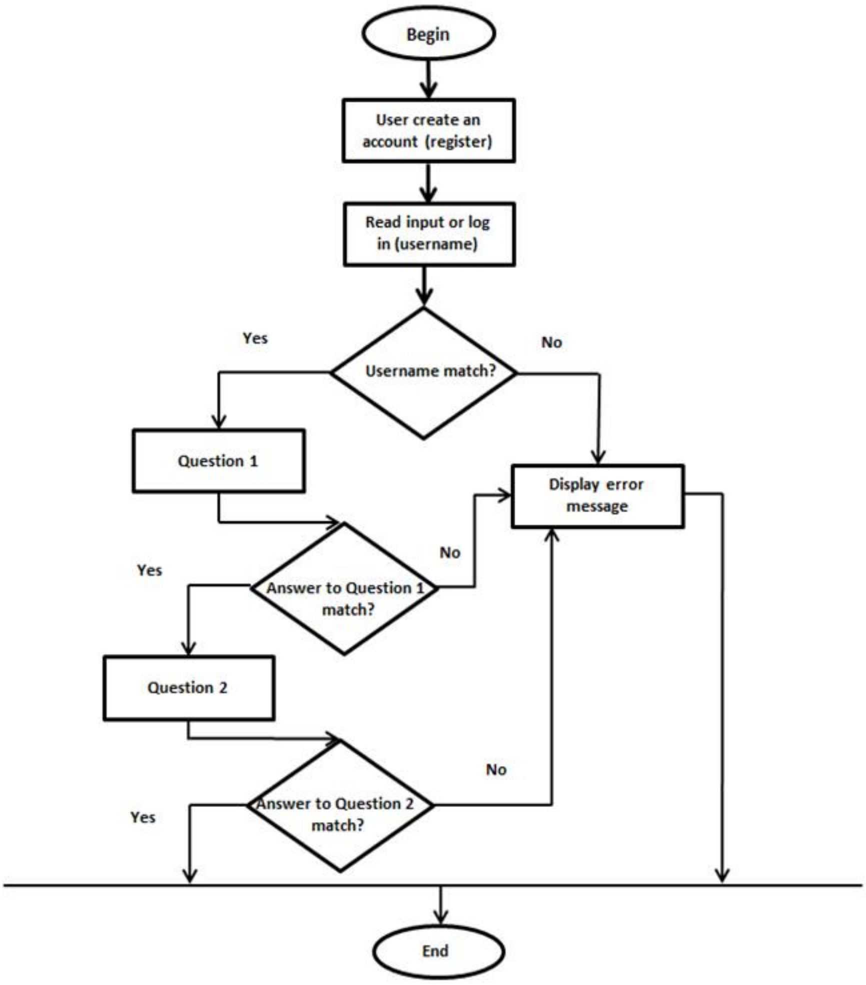

Begin
User create an account (register)
Read input or log in (username)
Yes
Username match?
No
Question 1
Display error message
No
Yes
Answer to Question 1 match?
Question 2
No
Yes
Answer to Question 2 match?
End

Figure 10. Knowledge Based Authentication (Ma and Feng, 2011)

All secret information is generated by the user during the registration process and is saved in the system's database, so that it can be compared with the user's input during later login attempts. The KBA is considered the most ubiquitous authentication approach used in distributed systems (Jørstad and Thanh, 2007). Even though passwords require inexpensive implementation and it is quite easy to manage them, they have several weaknesses. They are inconvenient, as they require memorisation, and some users have difficulty remembering multiple passwords (Jones et al., 2007), although research has suggested methods for creating strong passwords without reducing their memorability (Yan et al., 2004). Another problem with passwords is their vulnerability to attacks. Password cracking programs, some of which are available to download for free, make it easy to overcome passwords (Keith et al., 2007). Studies have reviewed various ways that KBA - both conventional passwords and image passwords - may be attacked (Summers and Bosworth, 2004; Towhidi et al., 2011; Rittenhouse, 2013). There are two commonly used types of KBA methods: static, which relies upon answers provided by the user, and dynamic, which generates both questions and answers from publicly obtainable information, typically via credit reports. Each presents distinct risk vectors, starting with the many drawbacks of static knowledge-based authentication (Baukes, 2018).

2.16.2. Token-Based Authentication (TBA)

A token is a piece of data created by the server containing information to uniquely identify the user. A new token is created for every token request, therefore there could be multiple tokens for the same user. Token-Based Authentication (TBA) is an authentication mechanism mostly used for authentication of API requests. In this mechanism, the user is issued an API access token upon successful authentication, which will be used while invoking any API request. In this process, a cookie will never be issued by the server. All requests are stateless (see Figure 11).

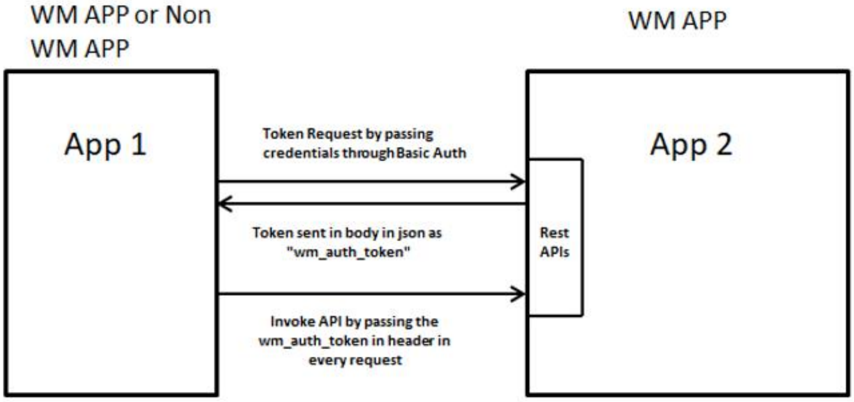

WM APP or Non WM APP
WM APP
App 1
App 2
Token Request by passing credentials through Basic Auth
Token sent in body in json as "wm_auth_token"
Invoke API by passing the wm_auth_token in header in every request
Rest APIs

Figure 11. Token-based Authentication for API Requests (Wavemaker, 2017)

The two categories of authentication tokens are contact tokens and contactless tokens. Contact tokens require physical contact between a token and a device reader, for example a magnetic strip on a card swiped by the user at an ATM. Another example of a contact token is a USB which must be inserted into a USB port on a computer in order to access a website (see Figure 12).

Figure 12. USB Token

The contactless tokens do not require physical contact with a reader. Instead they generate a new code, called a one-time password (OTP), for each authentication attempt. Examples of these tokens include secure device authentication, mobile phone authentication and card calculators (see Figure 13). OTPs avoid a number of shortcomings that are associated with traditional passwords. The most important shortcoming that is addressed by OTPs is that in contrast to a single static password, they are not vulnerable to replay attacks. This means that a potential intruder who manages to obtain a OTP that was already used to log into a service or to conduct a transaction, will not be able to re-use (or abuse) that OTP (SOPHOS, 2017).

Figure 13. OTP Generator

Mobile phone authentication is a relatively easy process for the user. The user gets sent a one-time password (OTP) over a separate communication channel (SMS or voice) than the IP channel (Internet) used by the application. The user then has to input this information into the application (see Figure 14). This provides security in case the IP channel is compromised (TNW, 2015).

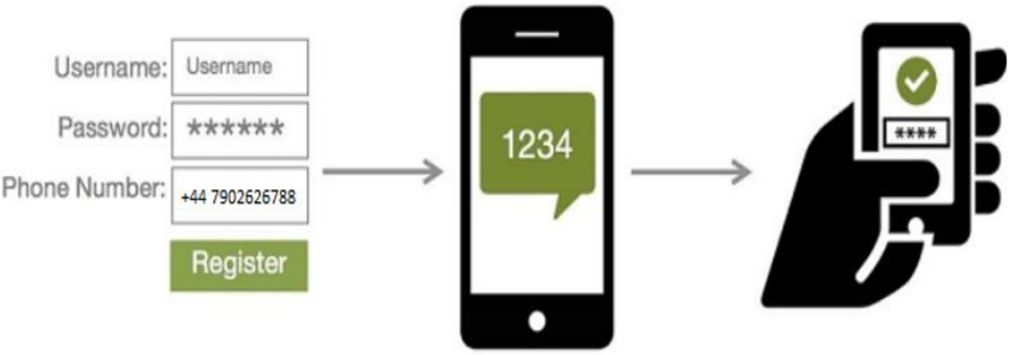


Figure 14. Mobile Phone Authentication

The user's phone number gets access to the password allowing him/her to log in to the application and verify their identity with an OTP or PIN code. The latter will create a verification relationship between the user and the system. The ubiquity of the mobile device, and the convenience of its utility as a one-time-use passcode device, will enable user to take advantage of the intersection of convenience and security.

The tokenisation is becoming widely being used in many transactional systems. For example, VISA Token Service, a new security technology from VISA, replaces sensitive account information, such as the 16-digit account number, with a unique digital identifier called a token. The token allows payments to be processed without exposing actual account details that could potentially be compromised.

If we compare TBA with KBA, the TBA provides more security, as all information is saved on the client side and the code that is generated by the token usually expires after a short period of time. However, tokens have their own disadvantages. For example, cost is involved: if one uses a USB token, it still needs to be purchased for every user; security can be very low: a token can be stolen or if a user keeps a USB token in the computer, which will revert a system back to a one-factor authentication system; ease of use and usability: USB tokens are very easy to use, but at the same time, USB devices break easily.

2.16.3. Biometrics-Based Authentication (BBA)

The use of physiological and behavioural biometrics to verify users' identities is called Biometrics-Based Authentication (BBA) (Renaud, 2004). A number of biometric methods have been introduced over the years, but few have gained wide acceptance (Kay, 2005):

- Signature dynamics. Based on an individual's signature, but considered unforgeable because what is recorded isn't the final image but how it is produced, i.e., differences in pressure and writing speed at various points in the signature.
- Typing patterns. Similar to signature dynamics but extended to the keyboard, recognizing not just a password that is typed in but the intervals between characters and the overall speeds and pattern. This is akin to the way World War II intelligence analysts could recognize a specific covert agent's radio transmissions by his "hand" -- the way he used the telegraph key (Rajesh, 2017).
- Eye scans. This favourite of spy movies and novels presents its own problems. The hardware is expensive and specialized, and using it is slow and inconvenient and may make users uneasy. In fact, two parts of the eye can be scanned, using different technologies: the retina and the iris (Mohamed, 2014).
- Fingerprint recognition. Everyone knows fingerprints are unique. They are also readily accessible and require little physical space either for the reading hardware or the stored data (Ezhilmaran and Adhiyaman, 2017).
- Hand or palm geometry. We are used to fingerprints but seldom think of an entire hand as an individual identifier. This method relies on devices that measure the length and angles of individual fingers. Although more user-friendly than retinal scans, it is still cumbersome (Bača et al., 2012).
- Voice recognition. This is different from speech recognition. The idea is to verify the individual speaker against a stored voice pattern, not to understand what is being said (Aladwan et al., 2012).
- Facial recognition. Uses distinctive facial features, including upper outlines of eye sockets, areas around cheekbones, the sides of the mouth and the location of the nose and eyes. Most technologies avoid areas of the face near the hairline so that hairstyle changes won't affect recognition (Lay, 2015).

However, there is a chance of errors and failures like any other authentication method. While BBA has a high degree of reliability, it costs much more than KBA or TBA. Kay (2005) reports that, while passwords represent an affordable and effective authentication method, they offer relatively little security. Security tokens must be carried by users and represent an additional layer of security. Although they are more expensive than simple passwords, they are much more affordable than biometric devices.

BBA is commonly regarded as the safest authentication method available, as it relies on a user's unique physical characteristics for authentication. The reliability of biometrics is increasing, as they depend upon characteristics that are unique to individual users.

According to BioLink (2017), fingerprint biometrics is the most popular, widespread, reliable and efficient biometric technology available today. Due to its versatility, fingerprint biometrics is applicable in almost all areas that require clear identification. Many notebook PCs and computer peripherals are coming to market with built-in fingerprint readers. Keyboards, mice, external hard drives, USB flash drives and readers built into PC card and USB plug-in devices are becoming available and they are relatively inexpensive.

This authentication method offers a high level of security against attacks, but the cost of implementation is high due to the high cost of the devices needed to read the biometrics. Additionally, not all users are willing to scan their characteristics; some may avoid laser reading, and others may have a medical phobia. User acceptance of biometrics varies, based on the type of biometrics. Fingerprinting, for example, seems to be more acceptable to users than face recognition and signature dynamics (Morales, 2010; Erden, 2018).

2.16.4. Location-Based Authentication (LBA)

Jaros and Kuchta (2010) stated that a user's location is considered sensitive information that can be exploited to identify the user. Denning and MacDoran (1996) were the first to propose the idea of using users' locations for authentication systems. The Location-Based Authentication (LBA) proposed by Denning and MacDoran (1996) is based on defining a unique, geodetic location for the user at a specific time, created using a location signature sensor (LSS) on microwave signals. The researchers claimed that this method of authentication would be 'extremely valuable' for 'financial transactions'; however, this authentication method has not yet been adopted. The increasing popularity of mobile phones has led to approaches that use them to establish user location and perform fraud detection. Park et al. (2009) propose a mechanism where the bank sends a message to the user's phone when he performs a transaction, including the details of the transaction and the location of the POS. A few researchers have improved the location-based authentication techniques (Jaros and Kuchta, 2010; Zhang et al., 2012; Ghodare et al., 2012). Recently, Marforio et al. (2014) used the trusted platform module (TPM) found on smartphones to sign

GPS coordinates, preventing a compromised device from supplying forged location data. This proposal is more robust as it uses the entire interconnected world instead of a single device to establish user location and augment authentication. Oluoch (2014) proposed a technique that works by comparing the location of a person's mobile device and where the log in attempt is being made. If the two match, then the log in succeeds, but if the two locations are different, the log in does not succeed.

The weakness of LBA is that it can be used to track users' locations all the time and in this case the user's privacy will be compromised. Moreover, this method requires the use of a Global Positioning system, which limits its usability with some applications. The use of location-based authentication is still under research and it is now being adopted in E-Learning.

2.16.5. Formula-Based Authentication (FBA)

In Formula-Based Authentication (FBA), which was invented by Ginzburg et al. (2006), a user is authenticated by finding the answer of formula. This technique is highly resistant to some attacks, e.g. SS (shoulder surfing attack) but sufferers from poor usability. In formula-based authentication, the user is presented with a mathematical formula containing values, characters and operators, and the user must provide the results of the formula for each login. The main advantage of this method is that, instead of entering a known password, the user is required to apply a formula that uses an unpredictable set of values and work out the result. What makes this authentication method particularly resilient is the fact the passwords change continuously and cannot be guessed without identifying the formula that generates them. On the other hand, the FBA may be perceived as time-consuming and inconvenient, because it requires users to obtain their chosen variable values in order to work out their passwords. Finally, this approach is not completely safe, as onlookers may still manage to deduce users' 'secret' variable parameters, especially if they are written down (Coulson, 2016).

2.16.6. Process-Based Authentication (PBA)

According to Shah et al. (2009), Process-Based Authentication (PBA) is a valid option which requires users to recall their passwords and perform certain calculations in order for the system to authenticate them. After entering their passwords or PIN codes, users are prompted to calculate an additional password on the basis of system-generated charactervalue combinations. According to Shah et al., in this method a user is authenticated using mathematical formula (password), containing characters (c), values (v) and operators (op). The user will memorise the formula and on each log in, he or she will provide the result of the formula by recalling the formula and then computing the answer of the formula. The user is not required to enter the actual password, but the result of the formula. This technique is highly resistant to over the shoulder attack, as it requires certain type of computation on the user side. Shah et al. claim that their approach is easier than FBA, as FBA requires users to have technical skills (Ferrag et al., 2016).

2.16.7. Risk-Based Authentication (RBA)

Among the many threats facing digital businesses including E-Learning, account takeover (ATO) is quickly becoming a problem. Forrester estimates that ATO causes at least $6.5 billion to $7 billion in annual losses across financial services, insurance, eCommerce, healthcare, gaming and gambling, utilities, and other industries (ThreatMetrix, 2017; Identity Automation, 2018). RSA (2017) suggests that risk-based authentication (RBA) identifies potentially risky or fraudulent authentication attempts by silently analysing user behaviour and the device of origin. RBA strengthens RSA SecurID authentication and traditional password-based authentication. If the assessed risk is unacceptable, the user is challenged to further confirm his or her identity by using one of the following methods:

- On-demand authentication (ODA). The user must correctly enter a PIN and a one-time tokencode that is sent to a preconfigured mobile phone number or e-mail account.
- Security questions. The user must correctly answer one or more security questions. Correct answers to questions can be configured on the Self-Service Console or during authentication when silent collection is enabled.

2.16.8. Digital Signature Authentication

Digital signatures are like electronic “fingerprints.” In the form of a coded message, the digital signature securely associates a signer with a document in a recorded transaction. Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance (see Figure 15). They are a specific signature technology implementation of electronic signature (eSignature) (DocuSign, 2017).

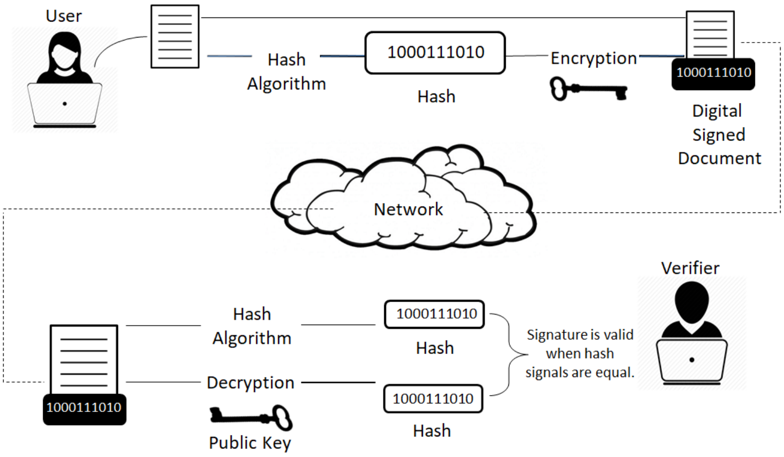


Figure 15. Digital Signature (DocuSign, 2017)

Digital signatures are the most advanced and secure type of electronic signature. You can use them to comply with the most demanding legal and regulatory requirements because they provide the highest levels of assurance about each signer's identity and the authenticity of the documents they sign. Digital signatures use a certificate-based digital ID issued by an accredited Certificate Authority (CA) or Trust Service Provider (TSP), so, when you digitally sign a document, your identity is uniquely linked to you, the signature is bound to the document with encryption, and everything can be verified using an underlying technology known as Public Key Infrastructure (PKI) (Adobe, 2017). A digital signature is built to prevent tampering. It is created, protected, and surrounded by the highest levels of security. The main reasons a user's digital signature is secure are outlined in Table 5.

Table 5. The main reasons why a user's digital signature is secure

Your digital ID is trusted	Compliant digital IDs come from accredited providers. The user needs to prove his/her identity before getting one.
It all gets encrypted	The user's digital signature and the document he/she signs are encrypted together and bound with a tamper-evident seal.
It is unique to user	Every time a user signs a document, he/she uses his/her own, unique certificate and PIN to validate the credentials and proves his/her identity.
It is easy to validate	Both the signed document and user's digital signature can be re-validated by a CA or TSP long after the signing event.

2.16.9. Mobile Pattern Authentication

Many researchers expressed the opinion that visual pattern recognition can play a key role in mobile applications for security check, context recognition and location detection (Himberg et al., 2001; Salah et al., 2002; Fritz et al., 2006; Bruns et al., 2007; Olade et al., 2018). Mobile devices are ubiquitous within our society (Von Zezschwitz et al., (2013). Today we depend on these devices to store substantial amounts of confidential information and perform activities such as social networking, personal internet banking, emailing and so on. Research by Mecaleff et al. (2015) shows that over 64% of users chose not to secure or use an authentication system on their mobile devices. The popularity of touch-screen based mobile devices allows for graphical authentication techniques that offer possibilities of providing passwords that are effectively stronger than text passwords (Olade et al., 2018).

The researchers further apply the mobile pattern authentication to medicine and other areas.

2.17. Comparative Analysis of Authentication Types

All authentication types are different. In order to understand the advantages and disadvantages in using authentication within E-Learning system, we have presented our findings by providing comparative analysis (see Table 6).

Table 6. Comparative Analysis of Authentication Types

Authentication Type	Advantages	Disadvantages
Knowledge-Based Authentication (KBA) (Ma and Feng, 2011; IDology, 2014)	• Password security is good if it is strong enough and provided by the institution • The set of questions must be answered within 5 minutes, which limits the risk of a fraudster researching answers.	• In the event that someone fails to answer the questions, they will be told to contact the company that sent the document to be signed. This is a security measure set in place to combat fraudulent access to an identity.
Token-Based Authentication (TBA) (Wavemaker, 2017; SOPHOS, 2017)	• More secure to use than user ID or passwords. • Enhance the image of the organization by securing user credentials more effectively.	• Involves additional costs, such as the cost of the token and any replacement fees • The token also expires after a set amount of time, so a user will be required to login once again. • Users always need to carry the token with them
Biometrics-Based Authentication (BBA) (Erden, 2018)	• Provide precise means of authentication: fingerprint, voiceprint, retinal design and DNA sampling. • Cannot be forgotten or lost (verifications associated with	• Environment and usage can affect measurements • Systems are not 100% accurate. • Require integration and/or additional hardware

	this authentication are highly individual to each user and are very difficult to steal or reproduce. • Reduced operational costs	• Cannot be reset once compromised
Location-Based Authentication (LBA) (Sharma, 2005;	• The location signature, that is, latitude, longitude (and sometimes altitude) adds a fourth feature to authentication factors and complements the current security methods. • A location record cannot be stolen and used somewhere else to acquire prohibited access, as it is almost impossible to replicate it.	• The accuracy of the GPS is critical to this scheme. • It will not work in the basements or inside of a big building where GPS signal strength is not good. • If the GPS is in a vicinity of tall buildings then signals might get delayed due to reflection providing inaccurate information. • The geometric positioning of the satellites at wide angles relative to one another is very important. • There is no GPS system integrity, that is, inability to inform users when the system is not reliable. • Orbital errors occur when satellites provide inaccurate information. • Cloudy sky and stormy weather adversely affect the potential of this technique.
Formula-Based Authentication (FBA) (Coulson, 2016)	• Instead of entering a known password, the user is required to apply a formula that uses an unpredictable set of values and work out the result.	• FBA is perceived as time-consuming and inconvenient; • It is not completely safe (as onlookers may still manage to deduce users' 'secret' variable parameters, especially if they are written down). • FBA requires users to have technical skills.
Process-Based Authentication (PBA) (Shah et al. 2009; Ferrag et al., 2018)	• This technique is highly resistant to over the shoulder attack, as it does not require to the actual password, but the result of the formula. • It is easier than FBA, as the latter requires users to have technical skills.	• It requires users to recall their passwords and perform certain calculation in order for the system to authentication them.
Risk-Based Authentication (RBA) (Identity Automation, 2018)	• Balances convenience and security • Risk threshold can be adjusted based on how your company defines risk • Can be used as a fallback to other authentication methods • Lower cost than other forms of strong authentication	• The system has to be maintained and updated as new threats emerge. Improper configuration may lead to unauthorized access. • The user's connection profile (e.g. IP Geolocation, connection type, keystroke dynamics, user behaviour) has to be detected and used to compute the risk profile. Lack of proper detection may lead to unauthorized access.
Digital Signature Authentication (DocuSign, 2017)	• It is created, protected, and surrounded by the highest levels of security. • Digital signature provides authenticity.	• The private key must be kept in a secured manner. The loss of private key can cause severe damage since, anyone who gets the private key can use it to send signed messages to the public key holders and the public key will recognize these messages as valid and so the receivers will feel that the message was sent by the authentic private key holder. • The process of generation and verification of digital signature requires considerable amount of

		time. For frequent exchange of messages, the speed of communication will reduce. • It does not ensure secrecy of the data. To provide the secrecy, some other technique such as encryption and decryption needs to be used.
Mobile Pattern Authentication (Mecaleff et al., 2015; Olade et al., 2018)	• Graphical authentication techniques offer possibilities of providing passwords that are effectively stronger than text passwords	• In case the device has been lost and stolen, it will be difficult for a user to log into the system straight awa.

2.18. Classification of Authentications

The most common authentication type in use is single-factor authentication. The single-factor authentication is a basic username and password combination. Most higher educational and business networks use basic username and password combination to allow access to secured or private resources.

Another form of authentication is two-factor authentication. The two factors of Two-Factor authentication are something you know (a password) and something you have (a token). The something you have factor can either be a token, a smart card, PIN/TAN and biometrics.

Tokens display a set of numbers, which changes every minute, on a small screen. This number is joined with the user's password, or PIN number to create a passcode. A correct passcode authenticates the user and will grant access to the secure resources. As tokens create passwords made up of longer streams of numbers to secure the system, it is considered a stronger authentication than passwords that must be shorter in order to be memorized (Bolle et al., 2003).

Smart cards are used in combination with a Smart Card reader. The user can insert the card and the card will send an encrypted message to the website, or the reader will display a unique code that the user needs to enter.

PIN/TAN stands for personal identification or transaction number. Consumers are provided with a sheet resembling a bingo card that contains many different numbers. Each number is used once to verify a transaction. E-signature and key-stroke dynamics not only record the final signature or word, but how the signature was either written or typed (Buss, 2005).

Biometric authentication uses biological aspects of the end user, e.g. fingerprints, iris scans, voice recognition, E-signature or key-stroke dynamics to provide authentication.

2.18.1. Single-Factor Authentication

Passwords are secrets that are known only to a user and are often combined with a username in order to gain access to a system. It is not a secret that passwords can be easily distributed, this authentication method is often considered inadequate to protect critical E-Learning activities from impersonation fraud (Apampa et al., 2008).

2.18.2. Two-Factor Authentication

No doubt that a user will not feel secured with long and complex passwords. Two-Factor Authentication provides a significant security over the traditional username and password combination. It is obvious that security of implementing some form of Two-Factor authentication is increased. The use of tokens, smart cards and key fobs are the primary second factor in Two-Factor authentication. As technology advances, biometrics are taking an important role to insure the identity of individuals trying to access E-Learning resources. In February 2011 Google announced two factor authentication, online for their users, followed by MSN and Yahoo. Using a Two-Factor Authentication process can help to lower the number of cases of identity theft on the Internet, as well as phishing via email, because the criminal would need more than just the users name and password details (Sarder, 2017).

A common example of two-factor authentication is an ATM card. In order to withdraw cash from an ATM machine, a person must first insert his credit card (something he owns) and then enter his PIN (something he knows). If he loses his credit card, he relies on the second factor (the PIN), to protect his credit card until he will notify the bank that the card is missing. Two-factor authentication works online in a similar manner to an ATM card and PIN combination. If a user wants to access an online account, he needs to use his username and password. However, after he successfully enters the correct password, instead of going directly to his account, the system requires a second factor authentication, e.g. verification code or fingerprint.

Bhargav-Spantzel at al. (2006) explored the use of two-factor authentication in an identity management system and stated that “the second authentication combines several authentication factors in conjunction with the biometric to provide a strong authentication”.

2.18.3. Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) involves the use of two or more independent security factors to authenticate a user. Multi-factor authentication is the most commonly used method of strengthening the login process in e-banking. Today 93 percent of organizations are using multi-factor authentication (MFA) to protect users and networks alike (SecureAuth, 2015). Organizations with more than 2,500 employees tend to opt for MFA over standard two-factor authentication, while companies in the 250 to 2,499 range are “very interested,” with 41 percent planning to implement or expand their MFA deployments (Bonderud, 2016). In 2014, Fujitsu introduced ground-breaking biometric systems authentication technology that uses the unique pattern of veins in the human hand to verify identity (Fujitsu, 2014). This new FUJITSU PalmSecure ID Match device protects access, data and payment. FUJITSU PalmSecure ID Match maximises physical security by allowing multi-factor identity verification, combining palm-vein technology and SmartCard with pin code option, for ‘real and true’ authentication to a very high level.

MFA has received its share of academic and scholarly attention, in part because the information in the context of higher education follows different norms than information that flows in and out of doctor’s offices and credit card company servers (Fordham IT, 2016).

2.19. Authentication Strength

According to O’Gorman (2003), authentication strength is measured by the combinations of the number and the type of authentication factors used to identify a remote system user.

The strength of authentication via password is very limited (Mehrabian, 1971). The first part of this combination, the username, does not seem to be insecure. However, in a single-factor authentication site, knowing the username, or even the current naming convention of the username within an organisation already give the potential hacker 50% of information required to gain access to vital information (Elrod, 2005). The problem of using a password for authentication is very obvious: what an attacker needs to do is just to guess or compromise a user’s password in order to gain instant access to the user’s online account and sensitive information. In addition to passwords, PINs and tokens are also weak authentications for deliberate impersonation fraud because they can easily be given out (O’Gorman, 2003). According to AltinKemer and Wang (2011), keeping complex passwords in mind in not easy and users are not willing to follow these rules.

Two-factor authentication still contains the inherent risk of impersonation because the user can distribute both the username/password and sign-on with a biometric match allowing the legitimate user to be impersonated (Bhargav-Spantzel et al., 2007). It is worth to mention that these days some technologies are already available to anyone to provide two-factor authentication. For example, Google account service. Anyone can request a two-factor authentication by simply setting it up under the account settings which can be accessed from any Google web applications. A free application is available for all the major smart phone platforms to generate the one-time passwords. It is named as Google authenticator. Therefore, it is a great opportunity to strengthen the Google account. Indeed, this process might seem to be a bit longer but it can provide a great level of security.

Many researchers expressed the importance of using the multi-factor authentication combining three authentication factors. Bolle at al. (2003) stated that it creates a stronger authentication improving reliability against impersonation fraud, Howell and Wei (2010) stressed the importance of using three-factor authentication in e-Finance and stated that "banks that have not yet addressed the need for multi-factor authentication should have that at the top of their [information technology] priority lists", Al-Khouri and Bal (2007) agreed that three-factor authentication is essential for e-Government and e-Commerce activities, as it "addresses the need for strong user authentication of virtual identities". Rodchua et al. (2011) stated that "creating multifaceted layers of devices can be an appropriate approach for the implementation". In 2015, Internet2 organisation was running a two-year project MFA "Cohortium" in the United States. The Cohortium is for gathering and creating as much information as possible around the business and use cases for multi-factor authentication in higher education (Jordan, 2015). The MFA "Cohortium" consists of 50 institutions and each institution is offering multi-factor on a voluntary basis to faculty and staff only. The project has helped fund software that makes it easy for an institution to plug in whatever multi-function authentication technology they want to use into that single sign-on system. It also enables institutions to switch small batches of users, instead of forcing everyone to switch over at once. The MFA "Cohortium" consists of 50 institutions

2.20. Copyright in E-Learning

Copyright is a legal right that protects the use of work once the idea has been physically expressed (BBC, 2017). The current copyright legislation in the UK is the Copyright, Designs and Patents Act 1988 (CDPA). The CDPA states that "where a literary, dramatic, musical or artistic work, or a film, is made by an employee in the course of his employment, his employer is the first owner of any copyright in the work subject to any agreement to the contrary". According to Strauss (2011), some claim that copyright applies to academic employees and therefore the copyright in teaching materials belong to universities. However, it is not always the case, as others claim that the academic/university relationship is typical and therefore the Act would not apply (Pila, 2010; Rahmatian, 2014).

The legislation alone does not address all the pertinent issues around the rights ownership of E-Learning materials. For example, when an employee leaves the institution /or organisation, what happens and who owns the legitimate right of ownership of the E-Learning material that has been partly developed by non-employees whichever case may be, and where are the students' involvements specified in the copyright agreement? The importance of copyright ownership by institutions /or organisations was first emphasized by Lape (1992) stating that it is important for universities to have effective copyright policies that address current and future issues relating to ownership of E-Learning material.

The issue of intellectual property rights (IPR) is one of growing importance and increasingly permeates discussions among E-Learning experts (Duncan and Ekmekcioglu, 2003). The E-Learning programs are complex and expensive; however, the legitimacy of ownership can be difficult to prove as the Internet boundaries cannot be questioned. The E-Learning materials represent valuable assets that need to be protected and managed. The management of the materials are solely based on trust that the person in the possession of the material will not give it or sell it to the third party.

The availability of versatile software and the inability to control the Internet have facilitated flaws in copyright of E-Learning content. Copyright is the most controversial area in E-Learning development. For the safety net of the E-Learning materials, institutions and organisations are applying watermarking. The watermarking technology can be classified under 3 main categories: copyright watermarking, integrity watermarking and annotation watermarking (Dittmann, 2000). Among the latter, copyright watermarking has been proposed and currently used by some institutions and organisations. Copyright watermarking is applied to secure ownership on copyrighted material, to detect originators of illegally made copies, to monitor the usage of the copyrighted data in any form and to analyse the data over networks and servers.

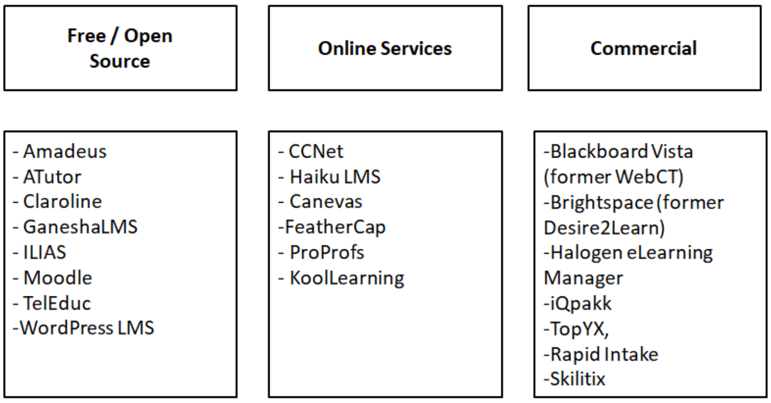
In reality, watermarking does not stop the illegal use or unauthorised alteration of materials. Any content that has been watermarked can be re-typed, printed and published in another language. Therefore, the research work shows that copyright is based on trust which should be emphasised by having a comprehensive policy in place that is openly available to all users.

2.21. E-Learning Applications and Security Vulnerabilities (case of Moodle and Blackboard)

The ubiquitous nature of E-Learning applications in dealing with a huge and diverse population of users creates the gap for errors and malicious attacks. The ability to quickly estimate security risks is particularly crucial for automated assessment of E-Learning. What type of measures is taken to keep the privacy and integrity of the information stored? Moreover, are there mechanisms that can prevent cheating when performing online examinations? In most cases, the E-Learning applications are designed and implemented to combine distinct services into a coherent whole in order to fulfil sophisticated tasks that cannot be fulfilled by a single service. Therefore, an awareness of threats and their countermeasures are essential, as E-Learning does not operate in a vacuum.

The architecture of E-Learning applications usually comprises of Web applications, Blogs, Games and externally visible properties. But, quite negligently the securities of the service that are going to establish the direct interconnections with others and invoke processes that are not involved are not often taken into consideration. Without doubt, the scope and complexity of E-Learning applications have grown significantly from small scale information dissemination to large-scale sophisticated systems that drive services and collaboration. The E-Learning applications are emerging as a standardized way to design and implement educational materials. These are implemented on standard platforms, therefore inherited similar security weaknesses that are published and available publicly. A major outcome of E-Learning process standardization is the common comprehension and execution of semantics that they provide.

Nowadays there are many Learning Management Systems (LMS) that are widely used in education. A Learning Management System (LMS) is an application that provides a comprehensive set of tools for educators to manage learning resources, administrative functions, assessments, and grading (Educause, 2010). The main types of applications can be divided in 3 main categories (Free/Open Source, Online Services or Commercial). Some of the applications that are used within the educational establishments and industry are highlighted in Figure 16.



Free / Open Source	Online Services	Commercial
- Amadeus	- CCNet	-Blackboard Vista (former WebCT)
- ATutor	- Haiku LMS	-Brightspace (former Desire2Learn)
- Claroline	- Canevas	-Halogen eLearning Manager
- GaneshaLMS	-FeatherCap	-iQpakk
- ILIAS	- ProProfs	-TopYX,
- Moodle	- KoolLearning	-Rapid Intake
- TelEduc		-Skilitix
-WordPress LMS		

Figure 16. List of Applications

All applications have common features, but some of them are more flexible and complete in specific aspects, such as role assignments, chats management, etc. Using E-Learning applications opens up an abundance of possibilities, but at the same time all applications open up to number of threats as students, private information, and resources become vulnerable to different types of attacks. The main attacks that Moodle and Blackboard are exposed to are described below.

2.21.1. Modular Object-Oriented Dynamic Learning Environment (Moodle)

Today everyone is familiar with Moodle (Modular Object-Oriented Dynamic Learning Environment). In the literature, Moodle is classified as E-Learning platforms. For example, this is how Moodle is defined online, “Moodle is a learning platform designed to provide educators, administrators and learners with a single robust, secure and integrated system to create personalised learning environments” (Moodle, 2015). However, in some sources Moodle is referred as a free application, widely used by many schools and higher institutions (Nagel, 2011).

As an open source, Moodle is exposed to many threats and vulnerabilities. Vulnerabilities can be detected early, however, they can also be exploited before patches are going to be available. Moodle does not always require users to re-authenticate due to session caching and does not restrict access though URLs. It is vulnerable to combined techniques of network monitoring (Spivey, 2007) and web-based attacks (Stuttard et al. 2007). We can divide these attacks in two groups, session attacks and design attacks.

The session attacks that are common to Moodle are Session Hijacking and Session Fixation:

- Session Hijacking

  Session hijacking is not an attack that gets a lot of professionals' attention. In recent years, the session hijack attack has been overshadowed by spyware, root kits, bot networks, and denial of service attacks. Session hijack attacks are defined as taking over an active TCP/IP communication session without their permission or knowledge. There are three different types of session hijack attacks; active, passive, and hybrid. The active attack is when the attacker hijacks a session on the network. The attacker will silence one of the machines, usually the client computer, and take over the clients' position in the communication exchange between the workstation and the server. The active attack also allows the attacker to issue commands on the network making it possible to create new user accounts on the network, which can later be used to gain access to the network without having to perform the session hijack attack. Passive session hijack attacks are similar to the active attack, but rather than removing the user from the communication session, the attacker monitors the traffic between the workstation and server (Nishanth and Babu, 2014). The primary motivation for the passive attack is it provides the attacker with the ability to monitor network traffic and potentially discover valuable data or passwords. The hybrid attack is a combination of the active and passive attacks, which allow the attacker to listen to network traffic until something of interest is found. The attacker can then modify the attack by removing the workstation computer from the session, and assuming their identity.

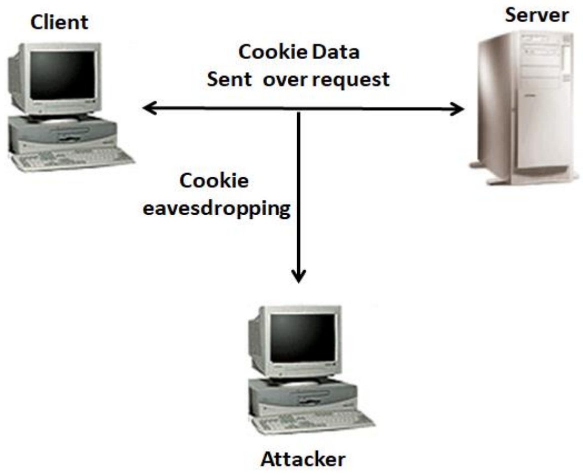


Figure 17. Session Hijacking

In case of Moodle, this attack is part of the eavesdropping attacks, where an attacker listens to the communication between client and server trying to find inside the payload (Arakelyan, 2013), in this case the HTTP request, information that can be used to impersonate the user and taking control of his or her session (see Figure 17). Moodle manages its session's trough two values to identify an active session: MoodleSession and MoodleSessionTest. These values are stored in the cookie that is sent on each HTTP request inside the header of the message. In order to impersonate a target user, an attacker must obtain such values. Obtaining a full HTTP request data with the cookie included is easy because Moodle only uses SSL tunnels on the login service and a few administrative services. For this reason, most HTTP requests are done on plain text that can be intercepted and easily decoded. After obtaining the cookie, the attacker can use this data on its own HTTP request, taking control of the target user's session.

- Session Fixation

  This attack also targets the session data of a user. Maiwald (2003) classified this attack as an active attack, where McClure et al. (2012) defined it as an interception attack (see Figure 18). Instead of eavesdropping the communication between a target user and the server, the attacker intercepts the HTTP request of the target user. Each time an anonymous user accesses Moodle, a MoodeSession and a MoodleSessionTest are granted. Therefore, an attacker can get such values as an anonymous user and then intercept a request of a target user that is not yet authenticated.

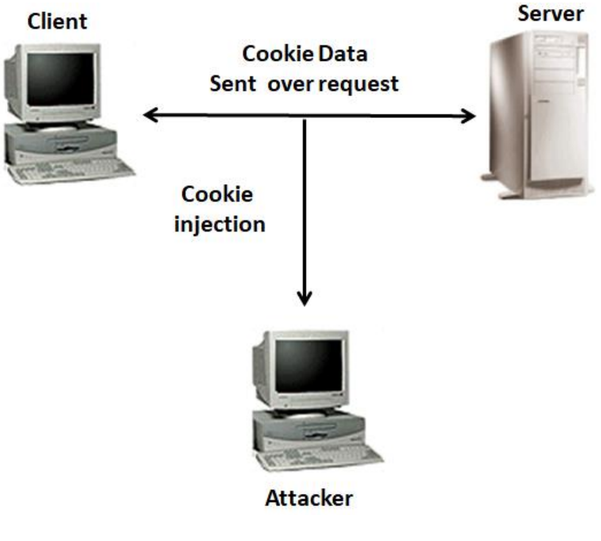


Figure 18. Session Fixation Diagram

Upon such an interception, the attacker replaces the user's MoodleSession and MoodeSessionTest values with those obtained previously. If the target user is authenticated, the session is granted with the user's permissions allowing the attacker to have the same permissions because he or she already has the MoodleSession and MoodleSessionTest values that identifies the fixated session (Arakelyan, 2013).

The most common design attacks in Moodle are Password Prediction and Username Prediction:

- Password Prediction

  The Password Prediction is done by sending multiple requests to the Moodle server with the cookie field empty. As Moodle has some flaws in design, the login failures count is reset to zero, while inside the request the cookie field is with no values or no cookie at all. It allows the attacker to perform a brute force attack for password prediction (Kumar and Dutta, 2011).

- Username Prediction

  This may be done by two methods: intercepting a cookie and by brute force.
  With the cookie intercepted, the field MOODLEID_was decoded with URL decoding and RC4 decoding. The private key for RC4 is hard coded inside the file moodlelib.php with the fixed value nfgjeingjk (Moodle ver. 1.8.6). Whereas the brute force method is used like in password prediction. However, instead of sending several passwords, several usernames are sent with a random password. The response from Moodle will take longer with a valid username than with an invalid one and this was used to differentiate between them in the attacks realised (Kumar and Dutta, 2011).

2.21.2. Blackboard

All LMS vendors acknowledged that no web-based software is perfect, and one should always expect to come across with vulnerabilities. In early 2010, Dutch security company Online 24 conducted a security research on Blackboard. During the research 84 different vulnerabilities were discovered within the Blackboard (Prins and Abma, 2010). Users of Blackboard were put at a serious risk. During the research 63 different cross-site scripting (XSS) vulnerabilities were found. All of these vulnerabilities could be exploited to hijack a user's session or even steal his/her login credentials. The most common types of Blackboard vulnerabilities were cross-site scripting and insufficient authorisation.

- Cross Site Scripting

The details of Cross Site Scripting (or XSS) were explained in sub-section 2.11.1. Figure 19 below shows the various types of vulnerabilities. The most common type, as seen in this chart, is the cross-site scripting vulnerability, followed by the insufficient authorization vulnerability. During the research two different types of cross-site scripting vulnerabilities were found: persistent XSS and non-persistent XSS. Persistent XSS means that the XSS vulnerabilities will persist after the request is submitted (e.g. it is permanently stored inside Blackboard). A non-persistent XSS vulnerability always needs special interaction between the user and Blackboard for successful exploitation and will not be stored anywhere (Prins and Abma, 2010).

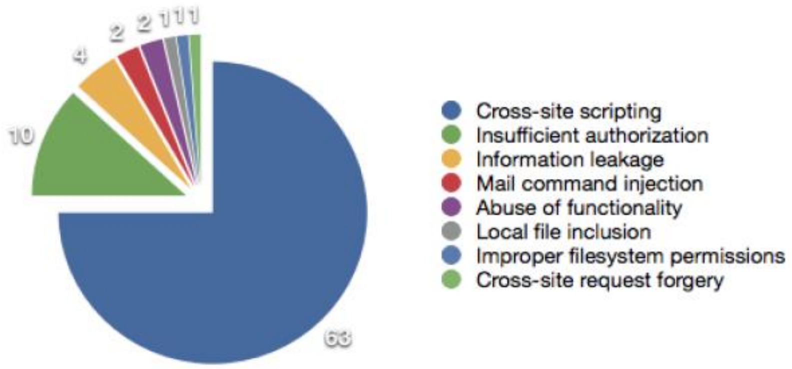


Figure 19. Types of Vulnerabilities (Prins and Abma, 2010)

- Insufficient authorization

  Insufficient authorization is the second most common type of vulnerability discovered during the security research on Blackboard, after cross-site scripting. During the research vulnerabilities were found which could enable attackers to read, modify or delete every Blackboard user's personal data (i.e. calendar items, preferences and address book items).

Furthermore, in 2011 multiple zero-day security vulnerabilities have been found in the world's most popular educational software. Zero-days have an average life expectancy of nearly seven years, with a quarter surviving over nine years (Hay Newman, 2017). Hoffman (2014) describes a zero-day vulnerability as "a hole or flaw in a software program for which there is no patch or fix, usually because the vulnerability is unknown to the software vendor". One Australian university, which declined to be named, recruited penetration testing company Securus Global to ethically hack the software. During tests of the Blackboard software, security professionals had gained administrative access to databases in which student exams, assignments and grades were stored. Personal information stored on students was also accessible. These vulnerabilities allowed students to change grades and download unpublished exams, whilst allowing criminals to steal personal information (Pauli, 2011). In Blackboard's security advisory and in interviews, they acknowledged that the majority of issues raised in Australia were valid security vulnerabilities. According to the stated Blackboard security and privacy policy, Blackboard cannot provide product updates according to a set timeline (Blackboard Privacy Policy, 2015). Blackboard planned to provide patches to Learn 9.1 "by the end of 2011" (Hill, 2011). This meant that the patches were available approximately 5 months after Blackboard was notified of the problems and approximately 3 months after the vulnerabilities became public in the magazine article and security advisory (see Figure 20).

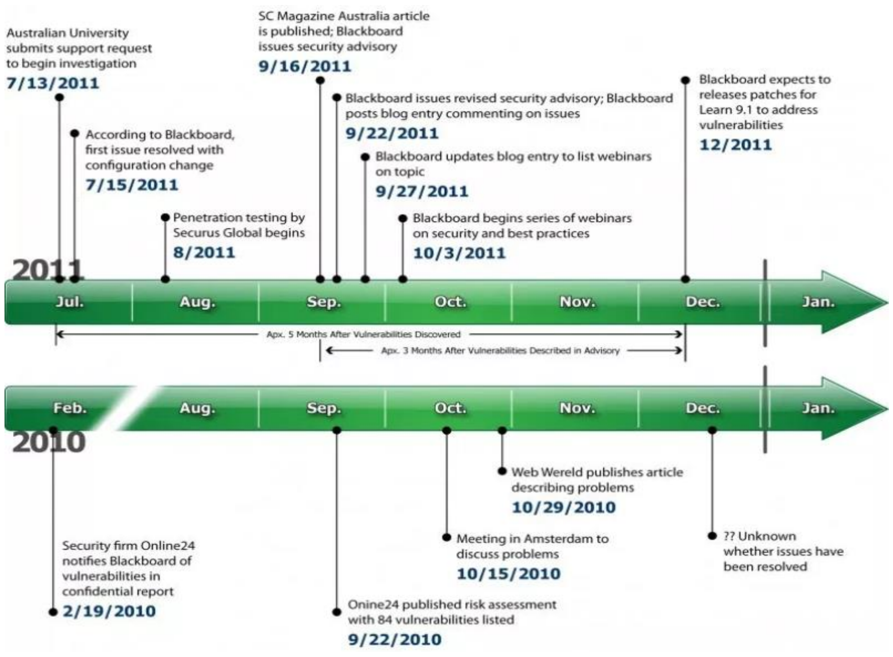

Australian University submits support request to begin investigation
7/13/2011
According to Blackboard, first issue resolved with configuration change
7/15/2011
Penetration testing by Securus Global begins
8/2011
SC Magazine Australia article is published; Blackboard issues security advisory
9/16/2011
Blackboard issues revised security advisory; Blackboard posts blog entry commenting on issues
9/22/2011
Blackboard updates blog entry to list webinars on topic
9/27/2011
Blackboard begins series of webinars on security and best practices
10/3/2011
Blackboard expects to releases patches for Learn 9.1 to address vulnerabilities
12/2011
2011
Jul.
Aug.
Sep.
Oct.
Nov.
Dec.
Jan.
Apx. 5 Months After Vulnerabilities Discovered
Apx. 3 Months After Vulnerabilities Described in Advisory
Feb.
Aug.
Sep.
Oct.
Nov.
Dec.
Jan.
2010
Web Wereld publishes article describing problems
10/29/2010
Meeting in Amsterdam to discuss problems
10/15/2010
?? Unknown whether issues have been resolved
Security firm Online24 notifies Blackboard of vulnerabilities in confidential report
2/19/2010
Onine24 published risk assessment with 84 vulnerabilities listed
9/22/2010

Figure 20. Timeline of Blackboard Vulnerabilities within Australian University in 2011 (Hill, 2011)

Without doubt, the above-mentioned vulnerabilities in the Blackboard Learn platform have the potential to affect millions of school and university students and thousands of institutions around the world. Securing Blackboard will be an increasingly important issue for institutions and industry, as web-enhanced and web-based delivery of educational content becomes more prevalent.

2.22. Classification and Taxonomy of E-Learning Security Threats

The classifications and taxonomy of E-Learning Security Threats are based on existing threats paradigm, which are specific to our research area. These threats are discussed in section 2.11. Over the past few years, we have seen evidence of an increasing number of people beginning to understand the concept of E-Learning Security Threats and the importance of Copyright, more specifically the delivery of educational contents. As a result, new technologies and ways of delivering educational material online have evolved, taking advantage of these new technologies. Based on the latter, users have become vulnerable to many E-Learning Security Threats which they have no previous knowledge of.

The security threats, that are associated to E-Learning systems, have led to our proposition of Classification and Taxonomy of E-Learning Security Threats (see Table 7). We focused on 5 major types of security threats that users come across while using E-Learning applications. They are: Cross Site Scripting (or XSS), Cross-Site Request Forgery (CSRF), Structured Query, Language (SQL) injection, Stack-smashing attacks and Session hijacking. These threats were described in sub-section 2.11. Each security threat has its concept and malicious results. We further broadened each type of security treats by adding 3 major categories which specify who are these threats in most cases committed by:

i. Steps-implementation of E-Learning Security Threats – These types of security threats are committed by novices, who have only or little knowledge about security threats. Most often they follow instructional steps detailed in YouTube and other online sources.

ii. Knowledge-based E-Learning Security Threats – These are mostly initiated by well-experienced or upcoming hackers, who are extremely knowledgeable to target specific area of the E-Learning system, possibly for the financial gain or to breach the Copyright Policy. The knowledge-based E-Learning Security Threats are extremely fast in propagation. This can affect thousands if not millions of users within a minute.

iii. Open-ended E-Learning Security Threats - These types of security threats are mostly committed by upcoming hackers. They can only spread within the E-Learning system and can be easily eliminated in most cases, as they do not spread so quickly. Open-ended E-Learning Security Threats mostly spread when a user copies the contents from where they have been contaminated.

Table 7. Classification and Taxonomy of E-Learning Security Threats

Types of Security Threats	Threat's concept	Malicious results	Steps-implementations of E-Learning Security Threats	Knowledge-based E-Learning Security Threats	Open-ended E-Learning Security Threats
Cross Site Scripting (or XSS)	• to manipulate client-side scripts of a web application to execute in the manner desired by the malicious user.	• accessing sensitive information; • identity theft; • altering browser functionality; • web application defacement; • denial of service attacks.	✗	✓	✗
Cross-Site Request Forgery (CSRF)	• to trick the victim into loading a page that contains a malicious request.	• logout; • purchase item; • change account information; • retrieve account information, or • any other function provided by the vulnerable website.	✗	✓	✓
Structured Query Language (SQL) injection	• to pass string input to an application with the hope of gaining unauthorized access to a database.	• check the user's input for dangerous characters like single-quotes; • using prepared statements, which tell the database exactly what to expect before any user-provided data is passed to it; • encrypt sensitive data; • ensure that error messages give nothing away about the internal architecture of the application or the database.	✗	✓	✓
Stack-smashing attacks	• to insert some attack codes (for example, code that invokes a shell) somewhere and overwrite the stack in such a way that control gets passed to the attack code.	• a web server or FTP server can be made to execute arbitrary commands.	✓	✓	✓
Session hijacking	• to gain unauthorized access to information or services in a computer system.	• the malicious attacker can enter the server and access its information without having to hack a registered account; • the attacker can also make modifications on the server that will help him hack it in the future, or to simplify a data stealing operation.	✗	✓	✓

☑ (Applicable) ☒ (Not-applicable)

2.23. Summary of Chapter Two

It is obvious that E-Learning receives a new meaning, as technology advances and business strategies change. E-Learning has come a long way in affecting not only academia but also businesses. Even though people benefit from E-Learning, it still has drawbacks that need to be taken into consideration. Most E-Learning innovations have focused on course development and delivery, with little or no consideration to privacy and security as required elements. Along with emerging technologies that are paving the way to the development and enhancement of E-Learning applications, the amount of threats and vulnerabilities increasingly grow. The effectiveness of any E-Learning application depends on how well the security aspects are incorporated in the system.

Privacy, Access Control and E-Learning system security management are currently one of the trending topics for researchers in E-Learning. Access control focuses on preventing unauthorized access to shared resources and meeting this requirement in E-Learning system is necessary in order to protect the content, services and personal data, but at the same time is very complex, as it can also affect the usability of E-Learning application.

Taking into consideration security requirements and also threats and attacks that are very common within E-Learning system, this thesis will investigate how Access Control can enhance security in E-Learning. As a result, a Dynamic E-Learning Access Control and Copyright Framework (DEACCF) multi-factor authentication method with biometrics will be proposed.

Chapter 3: Research Methodology

Introduction

Identifying the research methodology that best suits a research in hand is important, as not only as it will benefit achieving the set objectives of a research, but also as it will serve establishing the credibility of the work. According to Vaishnavi and Kuechler (2005), a set of activities considered appropriate to the production of understanding (knowledge) are referred to be research methodology. This chapter focuses on the methods, methodology and justifications for using the adopted approach in attaining the data and information required to prove or disprove the stated hypotheses in Chapter 1.

3.1. Research Paradigms

Research is described as a systematic investigation (Burns, 1997). According to Mertens (2005), the "exact nature of the definition of research is influenced by the researcher's theoretical framework". The theoretical framework, as distinct from a theory, is sometimes referred to as the paradigm (Bogdan and Biklin, 1998). Without opting for a paradigm as the first step, there is no basis for subsequent choices regarding methodology, methods, literature or research design. A research paradigm is a perspective about research conducted by researchers that is based on a set of shared assumptions, concepts, values, and practices. Saunders et al. (2012) emphasise the importance of the research paradigm in research as it is the framework which guides and supports how research should be conducted. Collis and Hussey (2009) identified methodology as the "overall approach to the entire process of the research study".

3.1.1. Positivism and Interpretivism

Rossman and Rallis (2011) identify 4 different paradigms (radical subjectivism, radical objectivism, interpretivism and positivism), of which the two primary paradigms are positivism and interpretivism, are outlined in Table 8. The latter paradigms are directly related to our research.

Table 8. Research Paradigms and Research Methods

Research Paradigm	Research Approach	Research Methods
Positivism	Quantitative	Surveys: • longitudinal • cross-sectional • correlational • experimental • quasi-experimental and • ex-post facto research
Interpretivism	Qualitative	• Biographical • Phenomenological • Ethnographical • Case study

- Positivism includes practical experiments in laboratories, field studies and surveys (Weber, 2004).
- Interpretivism is focused on case studies, ethnographic studies and phenomenological investigations, as they bear most effective results. The researcher interacts within the culture / participant that they are researching by using methods of informal interviewing, observation and establishing relationships (Creswell, 2011).

Weber (2004) believes that the differences between positivism and interpretivism lie more in the choice of research methods. He further suggests that different research methods and different data-analysis methods have different strengths and weaknesses, which provide different types of knowledge about the phenomena.

3.1.2. Deduction and Induction

There are two distinct methods of reasoning namely the deductive and the inductive approaches (see Figure 21):

- Deductive reasoning works from the "general" to the "specific". This is also called a "top-down" approach. According to Wilson (2010), a deductive approach is concerned with developing a hypothesis (or hypotheses) based on existing theory, and then designing a research strategy to test the hypothesis. Deductive approaches can be explained by the means of hypotheses, which can be derived from the propositions of the theory. In other words, a deductive approach is concerned with deducting conclusions from premises or propositions. According to Babbie (2010), “deduction begins with an expected pattern that is tested against observations”.

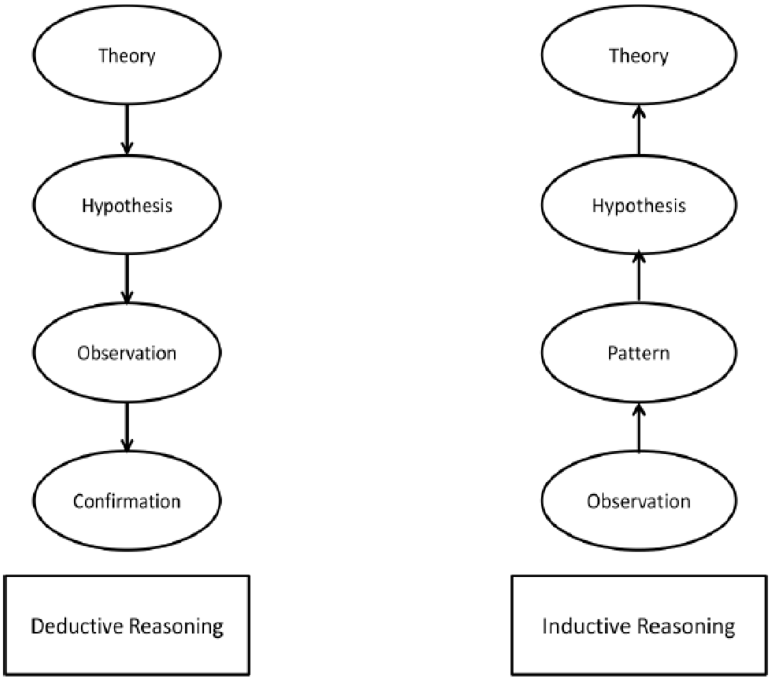


Figure 21. Diagrams of Deductive and Deductive Reasoning

Trochim (2002) explains the four stages involved in a deductive approach which starts with theory, refined into a hypothesis statement (null and alternative hypotheses), followed by observation, and ends with confirmation of the theory (see Figure 22).

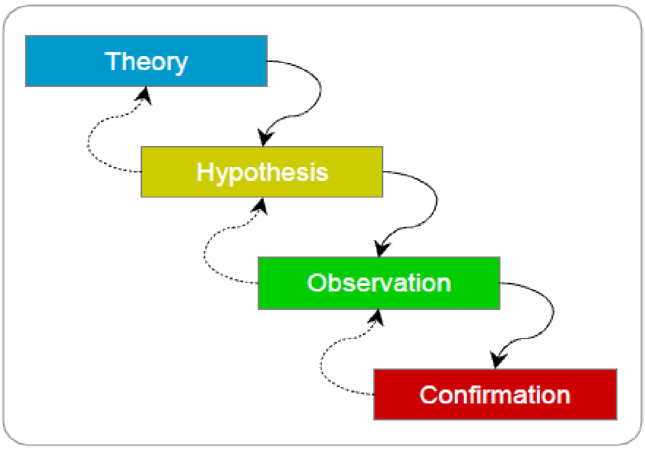


Figure 22. Deductive Reasoning Approach (Trochim, 2002)

- Inductive reasoning works from observation (or observations) works toward generalizations and theories. It is also called a “bottom-up” approach. Neuman (2003) states that inductive research begins with detailed observations of the world, and then moves towards more abstract generalisations and ideas.

The above-mentioned approaches are very different. Inductive reasoning is open-ended and exploratory especially at the beginning. On the other hand, deductive reasoning is narrow in nature and is concerned with testing or confirming hypothesis.

In the current study, the deductive reasoning approach is adopted instead of inductive reasoning approach. With the deductive approach it is possible to loop or cross check previous stages or findings within the study. This approach has been extremely iterative and also helpful. In contrast to inductive reasoning, deductive reasoning leaves no room for doubt.

3.1.3. Quantitative, Qualitative and Mixed Research Methods

Quantitative research focuses on quantification and analysis of data and is more aligned to deductive reasoning, whereas qualitative research focuses on words in order to generate theories and is more aligned to inductive reasoning (Bryman et al., 2011).

- **Qualitative Methods**

  Qualitative methods of investigation tend to be based on recognition of the importance of the subjective experiential 'life world' of human beings (Burns, 1997). Qualitative methods can produce a more in-depth analysis of a research area as it takes into account variables such as feelings, ideologies, environment and the complexities of the real world. The strengths of qualitative methods are that unexpected issues and findings can be established, with the scope of further exploration. A quantitative form of research follows a linear approach (see Figure 23).

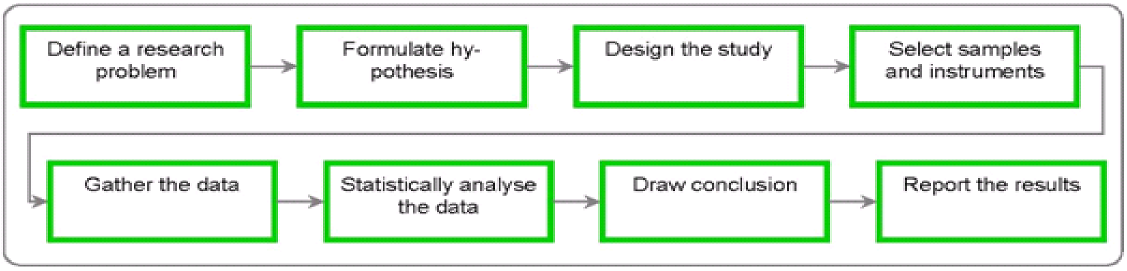

Define a research problem
Formulate hy-pothesis
Design the study
Select samples and instruments
Gather the data
Statistically analyse the data
Draw conclusion
Report the results

Figure 23. Quantitative Model (Burns, 1997)

The data is very descriptive and can establish relationships, causes and effects. The limitations that qualitative methods face are that they are very subjective and make the data gathered hard to validate. The data collected on a subject matter from one source may be contradictive and vary from the data collected from another source on the same subject matter. However, this does not make the result invalid. In qualitative studies, research methods are set up which suggest the type of methods of observation which may be used and the type of data which may be collected.

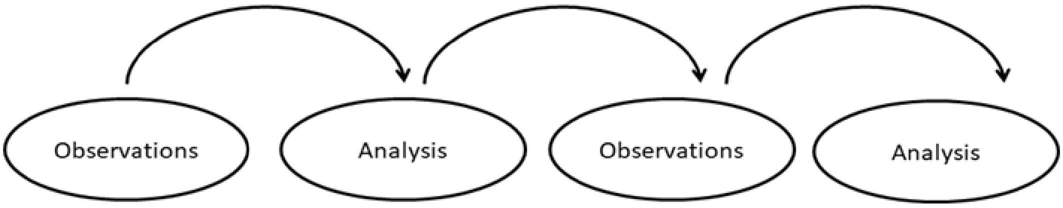


Figure 24. Research within Qualitative Studies

Analysis begins as soon as data begin to be collected. Analysis and data collection proceed in a cyclical fashion, where preliminary analysis informs subsequent data collection and so forth (see Figure 24).

- **Quantitative Method**

  Quantitative research is normally deemed as the scientific approach. In quantitative research, the investigator identifies a research problem based on trends in the field or on the need to explain why something occurs (Creswell, 2011). This involves a strong degree of control and precision, which is achieved through sampling and design. Experimentation is conducted which leads to statements about causation and effect. Quantitative data provides statistical analysis, which supplies answers that are much more concrete than a person's belief, opinions or intuitional views on a subject.

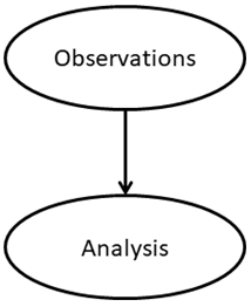


Figure 25. Research within Quantitative Studies

In quantitative studies, the research methods are set before observation begins and specify the methods of observation which may be used and the type of data which may be collected. Observations are collected before analysis begins. After analysis is complete, no more observations are taken (see Figure 25). The most prominent problem that arises from quantitative methods is subject matters that require measurement of subjective entities and variables that are difficult to analyse, for example, areas where environment and human behaviour is a major aspect. Quantitative methods often can produce synthetic results that are not flexible in taking into account many changing variables. Table 9 shows the comparison between quantitative and quantitative data collection methods (Adopted from Burns, 1997). It highlights clear distinctions between the analytical properties of the two methods: the quantitative process is the easiest to analyse, whilst the qualitative process produces a richer depth of information and knowledge.

Table 9. Comparison of Qualitative and Quantitative Methods

Qualitative	**Quantitative**
Approach: **-** Assumptions - Reality socially constructed	Approach: **-** Facts and data have an objective reality
Variables: **-** Complex and interwoven - Difficult to measure events viewed from informant's perspective - Dynamic quality to life	Variables: **-** Can be measured and identified - Events viewed from outsider's perspective - Static reality to life
Purpose: **-** Interpretation - Contextualisation - Understanding the perspectives of others	Purpose: **-** Prediction Generalisation - Casual explanation
Method: **-** Data collection using participant - Case study observation - Structured and Unstructured interviews	Method: **-** Testing and measuring

- **Mixed Methods**

Researchers have been conducting mixed methods research for several decades. Using a combination of qualitative and quantitative data can improve an evaluation by ensuring that the limitations of one type of data are balanced by the strengths of another. In the last decade, its procedures have been developed and refined to suit a wide variety of research questions (Creswell and Plano Clark, 2011). According to Figure 26, mixed research can be viewed as incorporating several overlapping groups of mixed methods researchers or types of mixed methods research.

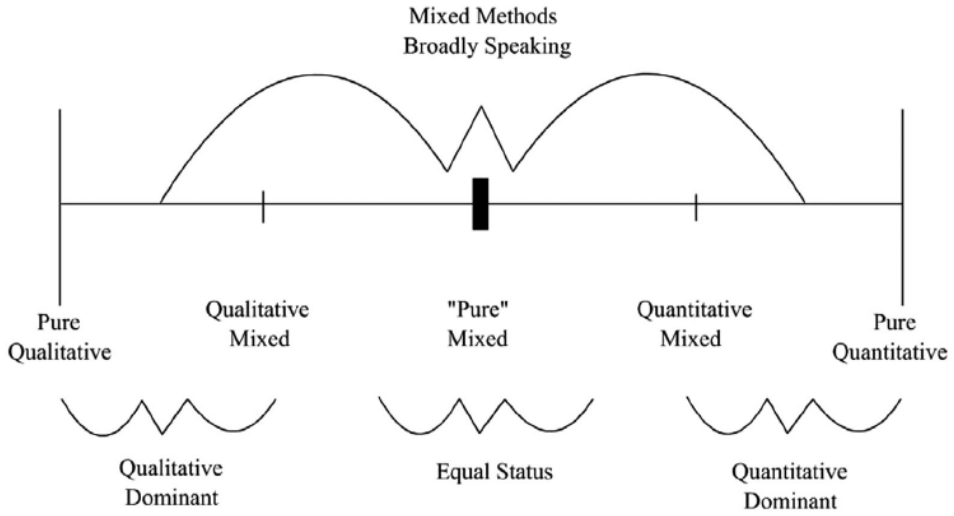


Figure 26. Three Major Research Paradigms, Including Subtypes of Mixed Methods Research (Johnson et al., 2007)

3.1.4. Summary of Research Paradigms

After analysing different research paradigms (positivist and interpretivist), the combination of qualitative and quantitative research methods will be adopted in order to better understand and explain the research problem. The positivist paradigm strongly relies on quantitative methods, in this research – questionnaire. The interpretivist paradigm relies on qualitative methods - case studies.

3.2. Data Collection Techniques

Data collection is the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions, test hypotheses, and evaluate outcomes. Research strategy is one of the components of research methodology. Research strategy provides overall direction of the research including the process by which the research is conducted (Remenyi et al., 2003).

3.2.1. Literature review

The literature review is our primary source of data collections, which would be analysed to explore some of the existing E-Learning issues. By literature review the accuracy of different existing theoretical findings can be verified, so as to deduce new ideas to carrying out this research and make sure these new ideas or findings are valuable as being based on reliable literature. Not only can the literature review provide a complete set of related theories from books, conference, papers, journals and research reports but give the up-to-date theoretical findings on the subject research area.

The secondary data will be reliable and convenient to analyse the theoretical findings because their accuracy has been proved by time and they are used in real projects. To strengthen the information found within the existing literature, a further research will be required. The primary source of data collection (quantitative method) will be used, because it will be vital for collecting data through the administering of questionnaires in the United Kingdom. Using quantitative method (questionnaires) will allow us to analyse the data collected using statistics in quantifying the results. These measures of statistics ranged from creating simple results and they shall be shown on tables. The latter will allow critical review of the subject area, hence directing the research. My data collection method will involve both quantitative and qualitative methods and the methodology that would be adopted within the framework of this study.

3.2.2. Questionnaire

The quality in design of the questionnaire is the difference between useful and useless data gathered.

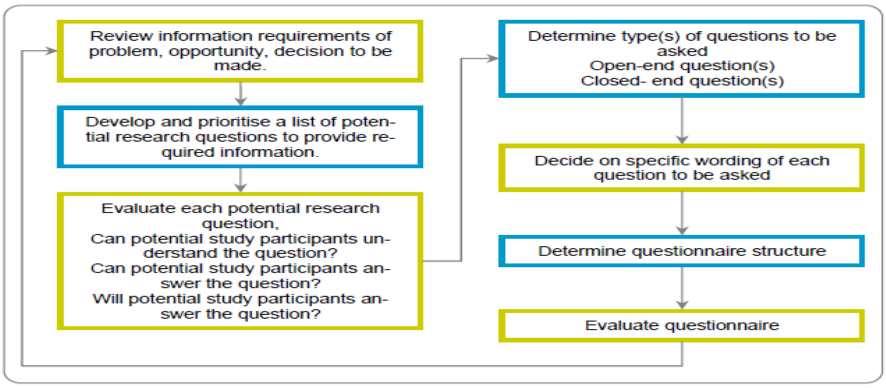

Review information requirements of problem, opportunity, decision to be made.
Develop and prioritise a list of potential research questions to provide required information.
Evaluate each potential research question,
Can potential study participants understand the question?
Can potential study participants answer the question?
Will potential study participants answer the question?
Determine type(s) of questions to be asked
Open-end question(s)
Closed- end question(s)
Decide on specific wording of each question to be asked
Determine questionnaire structure
Evaluate questionnaire

Figure 27. Steps in Constructing a Questionnaire (Peterson, 2000)

Suffice it to say, the term ‘garbage in and garbage out’ is quite fitting for the process of questionnaire design. Questionnaire construction is one of the most delicate and critical research activities (Peterson, 2000). The systematic approach proposed by Peterson in designing a survey questionnaire has been adopted (see Figure 27).

The questions in the questionnaire are carefully chosen to obviate ambiguity and to stimulate responses. Consequently, the survey questionnaire questions are a mixture of closed and open questions. The questionnaire has six sections:

- General information
- The impacts of E-Learning on the delivery of your programme(s)
- Risk assessment model for assessing the risk of E-Learning system
- Contents and Usage
- Security Measures
- Social Awareness

Attempts have been made to take out any inconclusive questions or questions that put potential respondents off, or questions that made the questionnaire time consuming to complete after gaining feedback from the initial pilot.

To avoid inherent bias in the questions, both open-ended and closed-ended questions are adopted. They provide aided recall by supplying a list of possible answers (e.g. the possibility of excluding possible responses):

i. Open-ended questions: The open-ended questions present the recipient with the flexibility in answering in any way they see fit to do so. This type of question does not restrict the participant by the questionnaire supplying possible answers to the questions in which one would have to be selected. Open-ended questions provide a wealth of information on a subject. The negative side to this is that it is hard for interpretation of statistical data. The positive aspect is that it allows a deeper understanding of what the respondent’s views and feelings are on the subject. There are situations where the open-ended questions are the only format that can be used in the questionnaire, for example ‘How many people does your company employ?’. Open-ended questions take less time to construct due to the absence of having to create the answers.

ii. Closed-ended questions: The closed-ended question restricts the participant to a number of possible answers that are documented within the questionnaire. This type of question can be viewed as an open-ended question with answers provided. This type of question requires the researcher to have a large degree of knowledge of the subject matter before the questionnaire is administered. For the reasons stated closed-ended questions require more effort to construct than open-ended questions, which were integrated into the questionnaire in this study.

Careful consideration is given to the design of the questions in order to avoid bias. Biased questions in a questionnaire make one response more likely than another, despite the opinion of the questionnaire participant. Bias can occur within the questionnaire design if there is a failure to supply adequate amounts of response or illegitimate answers to closed-ended questions. We make allowances for 'Any other Comment' at the end of some of the questions to enable respondents to include any response they feel is important, but is not included in the list of questions. The overall rationale is to increase the response rate. The questionnaire is an invaluable way to collect data and information, asking questions is perhaps second only to observation as the way people acquire knowledge (Peterson, 2000). The reasons for using a questionnaire survey for this research are detailed below:

i. Cost, questionnaires are amongst the cheapest form of collecting data for research
ii. Useful, when administered appropriately, information received can be valuable
iii. Each respondent receives an identical set of questions, phrased in exactly the same way
iv. Fear and embarrassment, which may result from direct contact, are avoided
v. The respondents are able to answer question at their own convenience
vi. E-mailing questionnaires can reach a wide variety of subjects over large geographical expanses
vii. A questionnaire that assures confidentiality to a user can obtain a more sincere response than a face-to-face interview
viii. The questionnaire is an unbiased way for the administrator to gather information.

3.2.3. Pilot Study

The participatory pilot study was conducted by involving 25 post-graduate students, 30 senior lecturers who were specifically coordinating E-Learning programmes (25 from universities and 5 from colleges) and 30 professionals working within the E-Learning system. All the respondents were UK based. They were asked to share their reactions, comments and suggestions in relations to the questionnaire.

The two limitations encountered in our pilot study were as follows:

- There were delays in getting feedback from the respondents.
- The time-consuming process to source out people who were willing to take part in the pilot study.

Based on the feedback of our pilot study, Questions 3 and 8 were restructured.

3.2.4. Sample Size and Method of Selection

An interpretative epistemology was considered the most appropriate perspective from which to gather information about security issues in E-Learning, actions and experiences with regards to the use of E-Learning. There are various formulas for calculating the required sample size based upon whether the data collected is to be of a categorical or quantitative nature (e.g. to estimate a proportion or a mean). Our research is based on the quantitative approach. The latter require knowledge of the variance or proportion in the population and a determination as to the maximum desirable error, as well as the acceptable confidence level and error risk. To determine the sample size needed, we referred to the Research Advisors (2006) as a guideline in choosing our sample size. It was stated that for a population size of 1000, the expected confidence level should be 399 questionnaire survey feedbacks. Our research population size exceeded the 1000 benchmark by 2370, in total we have a population size of 3370 with confidence level of 400 questionnaire survey feedbacks (see Chapter 5).

3.2.5. Case Studies

A case study is an in-depth exploration of a bounded system (e.g., activity, event, process, or individuals) based on extensive data collection (Creswell, 2011). “Bounded” means that the case is separated out for research in terms of time, place, or some physical boundaries. Yin (2003) defined case study as an “empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident”. According to Kane and O’Reilly-de Brun (2001), the case study observations allow the collection of data and presenting of information in a way that provides more context; they are good for showing how something happens or works in a real-life situation. Easton (2010) also states that case study “involves investigating one or a small number of social entities or situations about which data are collected using multiple sources of data”. Evered and Louis (2001) identify two different paradigms of organisational research, and term the two approaches 'inquiry from the outside' and 'inquiry from the inside', whereby the former is characterised by the researcher's detachment from the organizational setting, and the latter by the personal involvement of the investigator in the research process.

In this study, a multiple case study approach has been used. In multiple case studies, each case is studied as if it is a singular study and is then compared to other cases. According to Mesec (1998), the analysis of each following case is built on the knowledge obtained in the analysis of the previous cases. The selection of multiple case studies therefore needs to follow this replication logic. The two approaches for establishing the replication logic in a multiple case design, that are outlined in Figure 28, are the literal replication and theoretical replication (Yin, 2003). Literal replication entitles choosing cases that have similar settings and are expected to achieve similar results. The theoretical replication approach is used when cases have different settings and are expected to achieve different results.

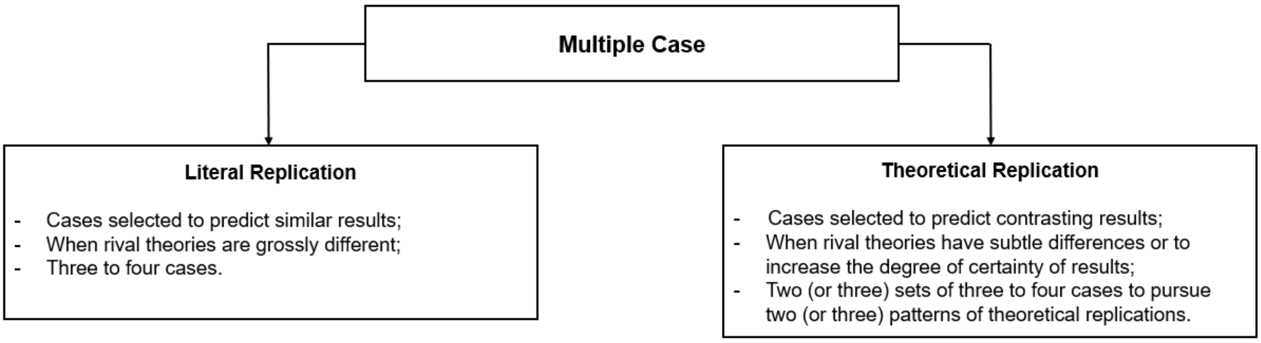

Multiple Case
Literal Replication
- Cases selected to predict similar results;
- When rival theories are grossly different;
- Three to four cases.
Theoretical Replication
- Cases selected to predict contrasting results;
- When rival theories have subtle differences or to increase the degree of certainty of results;
- Two (or three) sets of three to four cases to pursue two (or three) patterns of theoretical replications.

Figure 28. Selection Strategy for Multiple Case Design (Yin, 2003)

The satisfactory number of cases suggested by Yin (2003) should be between six to eight for a theoretical replication and three to four for a literal replication. For the purpose of this study, 6 case studies of E-Learning are investigated, so as to compare the limitations in each and see if the shortcomings will result into contrasting outcomes (see Chapter 4, sub-section 4.1.1 to 4.1.6.). Case study has multiple meanings, it can be used to describe a unit of analysis (a case study of a particular business), or to describe a method. The merits of using multiple case studies are to provide replication, logic and rich descriptions of emergent of this research, and to give concrete solutions to the problems associated with the failure of security in E-Learning.

The selected E-Learning case studies are used to identify data and information that were subjective and rich. It will highlight variables, processes and relationships that aided in the endeavours of this research.

3.2.6. Framework

Several information system researchers have pioneered the acceptance of design science research in information system. The study by Gregor and Jones (2007) describes design science as a sub-strand of a collection of constructive research approaches with a common emphasis of the central role of the artefact. Peffers et al. (2008) prescribe six processes for design science: identify problem, define objectives of a solution, design and development, demonstration, evaluation, and communication. A case for leveraging design theory to improve the transparency and rigor of design research is demonstrated by Piirainen and Briggs (2011) who integrate the framework in Hevner et al. (2004) and Peffers et al. (2008) as well as the design theory in Walls et al. (1992) with that offered in Gregor and Jones (2007). Patas and Goeken (2011) suggest interplay between behavioural and design-oriented research can be improved and draws a distinction between empirical and theoretical knowledge as well as non-artefact-centric and artefact centric knowledge.

Takeda et al. (1990) developed a cognitive model of design processes when examining a design process from a problem-solving point of view. This model is constructed from unit design cycles (see Figure 29).

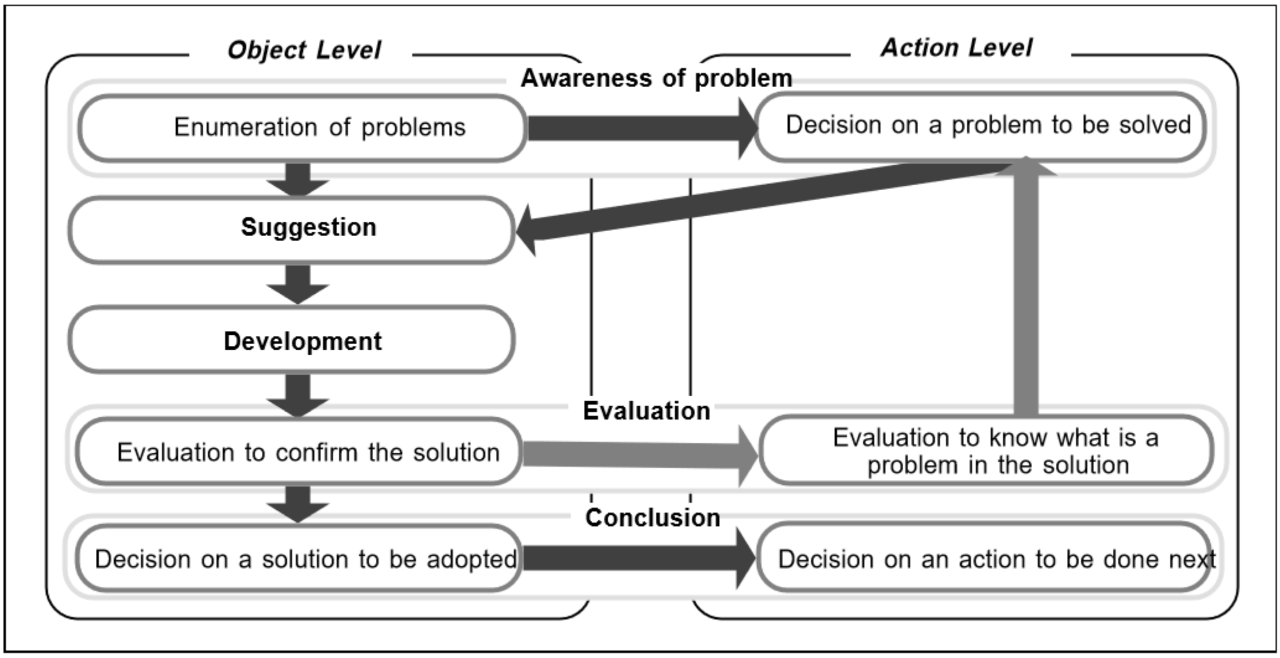

Object Level
Action Level
Awareness of problem
Enumeration of problems
Decision on a problem to be solved
Suggestion
Development
Evaluation
Evaluation to confirm the solution
Evaluation to know what is a problem in the solution
Conclusion
Decision on a solution to be adopted
Decision on an action to be done next

Figure 29. Design Cycle (Takeda et al., 1990)

A design cycle consists of five subprocesses:

(1) awareness of the problem: to pick up a problem by comparing the object under consideration with the specifications;

(2) suggestion: to suggest key concepts needed to solve the problem;

(3) development: to construct candidates for the problem from the key concepts using various types of design knowledge (when developing a candidate, if something unsolved is found, it becomes a new problem that should be solved in another design cycle);

(4) evaluation: to evaluate candidates in various ways, such as structural computation, simulation of behavior, and cost evaluation (if a problem is found as a result of the evaluation, it becomes a new problem to be solved in another design cycle); and

(5) conclusion: to decide which candidate to adopt, modifying the descriptions of the object.

The design science research processes that have been proposed by other researchers are outlined in Table 10.

Table 10. Comparative Analysis of Design Science Research Processes

	Takeda et al. (1990)	**Nunamaker et al. (1991)**	**March and Smith (1995)**	**Vaishnavi and Keuchler (2004, 2005)**	**Peffers et al. (2008)**
Problem identification	- Enumeration of problems	- Construct a Conceptual Framework		- Awareness of Problem	- Problem identification and motivation - Define the objectives for a solution
Solution design	- Suggestion - Development	- Develop a System Architecture - Analyse and Design the System - Build the System	- Build	- Suggestion - Development	- Design and development
Evaluation	- Evaluation to confirm the solution - Decision on a solution to be adopted	- Observe and Evaluate the System	- Evaluate	- Evaluation - Conclusion	- Demonstration - Evaluation

Based on our literature findings and the outcomes of the best fitted design science research processes to be adopted, we therefore opted for Takeda et al.'s cognitive model of design process (see Figure 29 and Table 10). An E-Learning security framework will be proposed from the short-comings envisaged in the quantitative and qualitative analysis results, weaknesses in the existing E-Learning Access Control (Chapter 2), analysis of six case studies observations and ten existing E-Learning models (see Chapter 4).

3.3. Summary of Chapter Three

This chapter outlines different existing research approaches and data collection techniques. The questionnaire survey and case studies are the preferred research methods because of the added advantages of incorporating elements of theory and implementation. Selecting respondents at random gave survey rooms for flexibility, in terms of ranging views of the people, rather than quota sampling that would have been based on gender or age. Furthermore, the sample of 400 was large enough for a research of this nature, given the time scale and the combination of research methods involved.

The combination of these methods satisfies the need for methodological pluralism and falls into both quantitative and qualitative research methods. It places the research within the context of existing knowledge and allows building new knowledge. Based on the literature review, questionnaire survey feedback and case studies, a Dynamic E-Learning Access Control and Copyright Framework (DEACCF) will be proposed.

Chapter 4: Analysis of Findings

Introduction

The E-Learning security problem has become a very important issue. Nevertheless, the availabilities of many defence mechanisms to prevent different types of attacks and the intrusion to E-Learning system have never stopped. Therefore, how to efficiently prevent the E-Learning security attack is an important research topic area. This chapter is focused on data collection and analysis of findings. It is achieved by analysing six E-Learning case studies, comparing ten existing E-Learning models and by conducting a questionnaire survey on Security Issues in E-Learning. After analysing the current techniques for securing E-Learning applications and Copyrights, a Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

4.1. Case Studies

The case studies used in this research are based on observation supported by literature reviews. The five case studies were selected for observation from the list of Ten Top UK universities ideal for distance learning (Pop, 2015) and one college from Best College Reviews (2015). The five case studies were the first five on the list of the ten top UK universities that are at the forefront of using E-Learning system to deliver all their courses and programmes and some with more than 80% of their programmes. While the college that was selected for our case study observation is the only college in the UK that fully adopted E-Learning applications to deliver 90% of the courses and programmes. For confidentiality and Data Protection Act (2018), the actual names of the universities and college are not disclosed. Instead, I have adopted to represent them by using alphabetical letters “Case Study Observation (CSO) A to F”.

After selecting the universities and college, I contacted each of their IT department via telephone and email asking for permission to spend 2 days to run my observations. I was also given the literature on how their E-Learning systems were developed to deliver the courses and programmes.

4.1.1. Case Study Observation A (CSO A University)

Background

The CSO A University serves a diverse region which ranges from city centres to traditional village communities. As part of the university's lifelong learning strategy, an out-reach service has brought ICT classes to adult learners unable to attend college classes.

The challenge

Many adults in low income groups or rural areas remain excluded from the digital revolution, yet ICT skills can offer access to information, a means of keeping in touch with distant relatives, and even a gateway to employment. Further education colleges have offered ICT classes in community venues for some time, but difficulties with broadband connectivity have restricted the range and flexibility of provision in rural areas, while learners' inability to travel has prevented them from joining campus-based classes.

Innovative solutions

In 2003, the college purchased a satellite communication van (the Satvan), capable of connecting to the Internet via the Global Positioning System (GPS) from almost anywhere. The Satvan can enable hard-to-reach learners to develop new skills on Internet-connected laptops in their own learning spaces – village halls, urban community centres, residential homes, and even the local pub.

A dedicated team arranges classes and plots the Satvan's route, ensuring it provides two or three classes per day over five days a week. A technician is employed to drive the van and set up the satellite communication, providing a broadband wireless link to the unit's 15 laptops. Working in their own environment to acquire skills in word processing, spreadsheets, Internet research, email and website development has proved very popular with learners. The results can also benefit the community as a whole: for example, creating a village website can involve all age groups in researching and promoting local amenities to a wider audience. The value of informal learning is that it removes boundaries: a group of older learners and staff in a sheltered housing complex, for example, have worked together to develop a booklet on the local town, Stow-on-the-Wold.

The technology

- SatWeb provides the broadband connectivity and 24 hour technical support for the satellite equipment used on the CSO A University Satvan. A GPS handset is used to locate the satellite.
- Network traffic is carried via the satellite between Tachyon Customer Premises Equipment (TCPE) and a hub (the Gateway). The TCPE is a terminal that connects subscriber sites into private and public networks and sits at the subscriber's site. The network is monitored and managed from a network operation centre and uses standard protocols and interfaces.
- Students use password-base authentication.
- Faronics™ Deep Freeze™ software has been installed on all laptops to restore standard Windows settings following class use.

Laptops will need maintenance every six to eight weeks; allow for at least one laptop being out of service for maintenance when taking bookings. Laptops can be affected by cold or damp conditions when stored in the van and are easily damaged in transit, so robust equipment is essential. Opportunities for learners to progress on to formal qualifications will be needed, where appropriate. A mobile laptop scheme can provide a means of bridging 'the digital divide' by ensuring that otherwise excluded learners have the opportunity to acquire ICT skills, and can feel part of a larger educational organisation. Other uses could include supporting remote rural businesses, promoting e-citizenship and capturing local knowledge to develop an oral history of an area. The use of better resourced IT suites in local schools may reduce the demand for mobile ICT training in the future. The resources could then be used to focus on the most disadvantaged categories of learners in urban as well as rural areas.

4.1.2 Case Study Observation B (CSO B College)

Background

The CSO B College, a general further education college, serves approximately 2,500 full time and 15,000 part-time students each academic year.

The challenge

In the mid-to-late 1990s, employers in South East London were experiencing a shortage of the technologically skilled workforce they required. College senior management saw that it was vital to contribute to a new vision for the town by creating a centre of educational excellence. The new build would offer a technologically sophisticated environment, which would enhance the effectiveness of learning and teaching, but also improve the efficiency of course management.

Innovative solutions

The South East London Centre was opened in 2003 with the aim of providing a state-of-the-art learning environment that would offer the best possible educational and training opportunities for the local community. The main entrance functions as a multi-purpose hall and reception area, known as the Atrium, which houses an Internet café, a learning shop and cubicles where guidance officers can provide information on career pathways and advice on a range of learning support needs. The centre now has 3,500 students using its facilities each day. Courses offered at the new South East London Centre include business studies, IT and science. All are now supported by a flexible suite of learning support options:

- Hubs of computers within a 'learning shop' encouraging independent learning, with support available where needed.
- The login is based on two factors authentication with smart card.
- Directed learning, where computers are arranged in suites, enabling groups of learners to follow instructions displayed on a screen.
- A learning development centre offering basic skills training.
- A mock office supporting elements of the business studies curriculum.
- Open access IT areas within the Internet café, providing recreational access to web-based resources and games for learners during lunchtimes and the evening.
- Computers, printers and scanners available within the learning resources area, enabling integrated use of print- and IT-based resources.
- Service loaning laptops on a weekly basis from the learning resource centre.

The aim has been to use the widest possible application of technology in support of 21st century learning and teaching. Teaching rooms are uniformly 'hi-tech' with interactive whiteboards, video data projectors, computers and DVD players and digital cameras as standard equipment. To maximise the use of the college's Virtual Learning Environment (VLE), and of other web-based and E-Learning resources in classes, access to the intranet and Internet is also possible in each teaching room. However, to offer the most flexible and responsive learning space, the college is also implementing wireless network access.

The guidance service has started to use mobile technologies to improve the reach and immediacy of its provision. Guidance officers have a visible presence in the newly designed Atrium at Stevenage; using wireless-enabled laptops and tablet PCs in discreet, screened off areas, they can provide access to a variety of support and guidance services for learners as they enter or leave the building. Formal interviews can then be arranged for a later date.

New builds are costly and, as a result, the efficiency of course management becomes a priority. A business process management system, Ultimus, has been introduced which allows mobile processing of information. With this, staff can act on business processes wherever they have access to a computer on any of the four campus sites or community outreach centres. The software also provides transparent measurement of process performance, which enables departmental managers to set service standards and create a culture of reliability and professionalism. The results have been positive. CSO B College has seen an 11% growth in student intake since the opening of the new centre, as learners have responded with enthusiasm to the technology-enabled environment.

The technology

To equip the Stevenage Centre, CSO B College purchased 520 Dell PCs for learners and for staff. Specially adapted computers and laptops with changes to keyboard size and mouse design have been introduced to support learners with disabilities. In order to ensure maximum integration of technology within the curriculum, it was decided to place a range of IT provision, from interactive whiteboards to data projectors, within every teaching room. Traditional resources such as overhead projectors and flip-charts are not made readily available. The management of the administrative processes within the college is undertaken with Ultimus business process management software. Staff and student portals and intranets are available for use alongside the VLE, Blackboard.

The administration and registration processes need to be efficient and effective to maximise return on investment. Business process management software can facilitate this, and should be considered. In order to fully adapt to teaching with technology, practitioners need to be confident in the reliability of the equipment and infrastructure. Technical support staff and training are therefore key to the success of a venture such as this − ongoing staff development in the use of IT, including mobile and wireless technologies, is vital.

A future aim is to provide every enrolled learner with a mobile device to access both in-house and external resources to support their learning, and to extend the use of SMS messaging. In time, it may be possible to send small learning objects and website links to learners' mobile phones to add value to what takes place in the classroom.

4.1.3. Case Study Observation C (CSO C University)

Background

The CSO C University in the UK has an undergraduate population of approximately 14,500. The Department of Mechanical Engineering is one of the largest in the UK, with some 500 undergraduate and 80 postgraduate students, and adopts a strategy of continuous improvement in its approach to teaching and learning.

The challenge

The first-year intake (approximately 130 students) into the department is normally amongst the most highly qualified at entry across the university. Yet despite their proven academic ability, it became apparent in the mid-1990s that students were having difficulty in acquiring understanding of the core curricular content, making 'inexplicable blunders' in the application of essential concepts. Furthermore, attendance at lectures and overall retention figures were dropping, an indication of low levels of morale. It was estimated that the department was losing almost 20% of its intake over the first two years of the course. There was also a further concern – that the rise in applications for courses in the department during this period would limit the potential for interaction with students, especially in the crucial first year of their studies.

Innovative solutions

As part of a wider project, New Approaches to Teaching and Learning in Engineering, or NATALIE, changes were introduced to the pedagogical approach used in the department. A product called Interwrite PRS (Personal Response System) from GTCO CalComp was adopted and four lecture rooms, seating up to 150 students, were equipped with PRS receivers and voting devices. In some of these rooms, curved rows of seats were installed to allow students to engage in group discussion while still facing the front of the theatre. The system can be accessed using password-base authentication on a USB stick.

The PRS is an electronic voting system. Students use handsets, which operate at a range of up to 60 ft. from the receivers, to respond to multiple choice questions using infra-red technology similar to a TV remote. Receivers are linked to a computer or laptop and a data projector, and software installed on the computer immediately converts responses to histograms or bar charts, facilitating further discussion.

With the introduction of PRS, the content of lectures was re-structured to focus on the establishment of core concepts and the testing of students' understanding in line with a social constructivist perspective. Students were asked questions based on background conceptual knowledge, then required to explain and defend their responses in the face of questioning by others with different perspectives. The approach can be broken down into the following stages:

- Introduction of a concept.
- Response to questions (individuals test their understanding).
- Polling of answers provides feedback (projected histogram shows group results).
- Peer discussion (individuals asked to defend their answer).
- Second vote (students respond again individually).
- Further feedback (histogram shows subsequent group response).
- Summary and explanation of 'correct' response by lecturer.
- Optional class-wide discussion.

Discussing conceptual questions in class with their peers has proved to be a powerful motivating force, perhaps because the new structure allows students time for reflection, but also because debate, discussion and questioning have been shown to support more active learning. Students feel motivated to focus on knowledge gained during a lecture so that they can perform well in what they see as 'fun' assessment activities. In a suitably structured lesson, the continued reference to tasks involving the voting system help to maintain a consistently higher level of student attention to the content of the lesson and promote thought about the issues raised. The PRS system has now also been adopted by staff in the Physiology and Pharmacology and Mathematics departments, and the French Studies division of the Department of Modern Languages.

The technology

The system comes with software which is installed on to the computer or laptop and enables student responses to the multiple-choice questions to be instantly displayed. The Interwrite PRS software also has a 'Review Session' feature that allows the lecturer to see the results of a questioning session both on an aggregate basis and by individual student. In addition, data from student responses can be imported into a variety of other applications including Notepad, Microsoft Excel and Word. InterWrite PRS software is an independent application that operates on Windows or Mac OSX platforms and can easily import graphics for PRS-generated questions. The hardware proved to be simple, reliable and inexpensive (approximately £1000 per 100 students). Receivers operate on a line of sight and so do not interfere with radio frequency equipment or systems in adjacent rooms. Other similar systems exist but may have different features and capabilities. It is important to check that the chosen system will support the number of potential users in large group settings. Mobile PRS units will make the system more widely available, but its use will have effects on the timetable: two hours rather than one-hour sessions will be needed to enable group discussions to take place. As a result, not all curricular content can be covered in class.

The use of PRS has been fully evaluated. This revealed that students interact with lecture content and with each other in a number of different ways when using polling devices and that the variation in techniques stimulates learning still further. Results from diagnostic tests provide further evidence of raised standards in the department. The retention problem has been greatly reduced; exit interviews with those leaving show that lack of motivation is no longer cited as a cause.

4.1.4. Case Study Observation D (CSO D University)

Background

The Interactive Logbook was developed as a research project within the Centre for Educational Technology and Distance Learning (CETADL) at the CSO D. The EU has awarded funding for its further development; the Interactive Logbook is now available for UK-wide trials in higher and further education institutions.

The challenge

In order to work in small groups on collaborative projects, access to online learning resources and lecture notes is needed. Students also need to be able to create, share and amend documents in real time, keeping a record of activities and achievements for personal development planning and portfolio-building purposes. Field studies have shown that existing personal information management tools offer only some of the functionality required for educational use at a higher level, and do not always integrate well with Virtual Learning Environments (VLEs), portals or other online systems, or different makes of software.

Innovative solutions

The aim was to design a flexible suite of software applications optimised for use on tablet PCs which, in conjunction with a secure wireless local area network (WLAN), could support student learning in a variety of settings – lecture theatres, libraries, common rooms and individual workspaces. Currently available plug-ins include:

- Log-writing tool for personal development planning
- Email
- Microsoft Office
- OpenOffice
- SharePoint Portal client
- Multimedia notebook
- Organiser
- Chat
- File manager
- Web browser
- Group account with password-based authentication.

This combination allows a user to create and manage files, view appointments, use synchronous or asynchronous communication tools, store personal notes and documents, and access learning resources via a wireless connection to the network whenever needed. The open architecture allows additional software to be added as required. Installed on a tablet PC, the Logbook will support learning tasks involving discovery, problem-solving, collaboration and the sharing of resources. Taking a personal device wherever you learn encourages a sense of ownership of learning and increases control over the learning process, building evidence for personal development planning.

The technology

The Logbook has been developed for the Toshiba Tablet PC which runs Windows XP. As portable as a laptop, a tablet weighs a little over 1.4 kg, has a battery life of 4–5 hours and offers ease of use in different contexts, i.e. standing as a well as sitting. The Logbook software can be run in any Windows environment, including desktop computers. The Logbook's applications are located within four main sections on the screen's launch panel:

- 'Programs' – providing access to the Internet and applications such as text messaging, freehand notes, PowerPoint
- 'Modules' – providing access to teaching materials using group account.
- 'Meeting' – providing access to collaborative tools such as a peer-to-peer whiteboard session.
- 'Diary' – providing time management facilities.

The tab panel at the bottom of the screen gives access to shared group and personal resources. Key elements of the software (such as diary management) will also be made available in the future on smaller mobile devices such as Java-enabled mobile phones, and integrated with the Logbook software. Induction for students and practitioners will be needed to develop appropriate uses of the Logbook. Practitioners may also need to be prepared for increased demand in online learning resources. Costs of implementation may be reduced as the number of students using their own mobile devices increases. However, loan schemes will be needed for the foreseeable future.

Installed on a tablet PC, the Logbook software will support learning tasks involving discovery, problem-solving and collaborative learning. Use of the Logbook by students in lectures and seminars could also speed up their understanding of concepts and prepare the way for assessed group work.

4.1.5. Case Study Observation E (CSO E University)

Background

The University Library and Learning Services at CSO E University are responsible for library and learning support services on two campuses, IT open access areas across the university (including those within the libraries), IT training, and information literacy programmes and materials. The City Campus Library, situated at the heart of the city, is the larger of two libraries, with approximately 1.1 million visits per year.

The challenge

The City Campus Library, opened in 1978, had received little investment in buildings or infrastructure, and the facilities available were increasingly unable to sustain the demands of a learner-focused library service. By mid-2004, only 39 of its 1050 study seats were equipped with open access IT. Key constraints were the lack of appropriate access control (use only password-based authentication), ventilation and networking infrastructure. However, student demand for access to IT had been rising significantly. Facilities were being used at full capacity for the duration of the library's opening hours with queues regularly forming at peak periods. This was in spite of additional facilities provided in the two open access IT centres at City Campus. Furthermore, changes in assessment and pedagogical approach were clearly impacting on students’ use of learning materials. An increase in assessment of group work and changes in student culture indicated that redevelopment was necessary. Increasingly, students were seeking access to resources on the Virtual Learning Environment (VLE), to web pages, e-journals, e-books and databases alongside print-based materials. User surveys had shown that the use of print and online resources had continued to increase at an equal rate, demonstrating that they complement rather than exclude one another, and should be offered in combination.

Innovative solutions

Factors such as these led the Library and Learning Services team to redefine the library in terms of a hybrid learning space. Accommodation has been reconfigured to provide a mix of resources and environments to match specific learning styles and outcomes. Designated areas are now zoned by use of colour and defined by permitted levels of discussion and refreshments.

Infrastructure

The university IT and Infrastructure programme identified the need to make the existing building fit for purpose by upgrading the power supply, ventilation, lift access and lighting to each of the 500 sq m floors. The university also approved reconfiguration of the existing IT and study space in the library basement, upgrading the group discussion and IT facilities to provide a range of attractive areas for relaxation, individual study and group discussion alongside refreshments. The library at the City Campus has now gained overall 130 open access workspaces which allow integrated access to print and online resources alongside desktop software and courseware. Although Floor One is mostly given over to study space with IT access, the design of the space and the use of furniture allows the technology to be used in a flexible manner i.e. within groups or individually, as an IT-only activity, or in conjunction with printed materials. Input from students was important when drawing up the designs. The flexibility and choice for students has also been extended by providing 30 wireless laptops on a loan system for use anywhere within the City Campus building. A consistent student desktop environment is provided, whether using a loaned laptop or a personally owned one, by virtue of Citrix technology (see below).

Support

IT Support and Enquiry Services team members are developing an integrated one stop support facility for students, encompassing what is currently offered at discrete IT support and enquiry service desks. With a new service structure developed, a learner support team will provide help with IT and library enquiries and support training and production of documentation to foster greater independence amongst students.

A smart card access system has introduced a balance of staffed and self-service opening hours. These now run from 8.30am until midnight Monday to Friday, 9.30am until 5pm Saturday, and 11am until 5pm Sunday. Before 9am and after 9pm the facilities are open on a self-service basis with security staff appointed to monitor the buildings and use.

Flexibility of provision

The existing learning space in the library basement was reconfigured to blend IT provision with casual seating – the result was the ‘Learning Café’. All work areas have access to power and to the Citrix desktop via a wireless virtual local area network (VLAN), and the area is designated a ‘green phone zone’, where mobile phones may be used on silent. There are no rules prohibiting food and drink whilst using the Learning Café facilities. The result is a social learning area which extends the options provided on Floor One. Integrated within it are individual and group working spaces to provide maximum flexibility for different kinds of learning and social activities.

The User surveys had provided evidence that academic tasks were being compromised by use of open access IT facilities for activities such as checking e-mail, web-browsing or online shopping. The Library and Learning Services staff believe that such activities are legitimate and must be supported, but not at the expense of other academic users. As a result, the concept of casual access points was introduced to meet this demand. These are short use IT stations which are supplemented by 'nomad points' within academic and other areas of the campus – these are positioned on a high desk so that users stand to access the IT, or sit at high benches for short periods of use.

The technology

- Citrix: This is a 'thin client' technology in which the applications are executed on one or more remote servers with only screen updates being transmitted across the network. This results in low bandwidth on the network, and allows applications to be used on lower specification terminals. This move enabled the university to run all applications on file servers and provided central management and configuration of applications and desktop environments, presenting students with the same 'look and feel' and the same access to resources whichever route they choose.
- Static workstations: 100 Neoware Capio One thin client static appliances were purchased providing access to the Citrix desktop and the university's VLE. These can be used in groups or individually.
- Casual access points: Additional Capio One thin client appliances are available within the Learning Café on tall stations where users stand or use high stools.
- Two specialist research hubs have been designed to offer high spec desktop computers and a screened private study area.
- Wireless laptops: A Cisco Wireless LAN Solution Engine is used to centrally configure, manage and monitor all of the wireless access points for the virtual local area network. Wireless cards need to be 802.11b compatible.
- USB Pens/'A' Drives/Mice: These are available for purchase or loan from the Learning Café shop.

It is important to ensure that utilisation of space is kept as flexible as possible in order to 'future proof' the infrastructure; involving academic staff and students in the design of learning spaces will help to ensure the effectiveness of the design. For example, non-pedagogical factors within the learning environment, such as levels of noise, lighting and heat, can be essential to students' ability to focus on higher order tasks and these requirements should be taken into account in any redevelopment.

Assumptions made about how and why students use IT need to be challenged – flexibility is paramount. A choice between types of learning spaces provides students with the ability to respond more effectively to differing study and assessment requirements at different stages in their programme of learning.

4.1.6. Case Study Observation F (CSO F University)

Background

The Interactive CSO F Laboratory received funding in 2003 to undertake the Sussex Mobile Interactive Learning Environments (SMILE) project with a mixture of postgraduates and third year undergraduates on the Interactive Learning Environments course. This is an optional course offered within the Informatics Department in the School of Science and Technology.

The challenge

The SMILE project had explored the application of the O2 XDA to an educational context – the XDA is a personal digital assistant (PDA) integrated with mobile phone features. Students were issued with these devices to use as their own during the project, to develop and evaluate their own collaborative and interactive learning experiences within a broadly constructivist pedagogical framework. However, this application of the XDA was outside of normal patterns of use, and resulted in time-consuming dialogues with the service provider and supplier. The start-up costs had also restricted the number of devices on offer. As a result, the undergraduates had to share devices with an average of one between three people. Despite reservations over the suitability of the combined mobile phone/PDA as a tool for this purpose, students had responded positively during the project to mobile access to essential resources, and tutors still aimed to encourage greater ownership of learning materials in digital format.

Innovative solutions

A tool which offered a simple, cheap and unobtrusive token-based authentication solution was the USB stick / storage device, sometimes known as a ‘pen drive’ or a ‘memory stick’. The CSO F Laboratory experimented with this simple technology by offering each student a 256 MB USB storage device to use during the spring term of 2004 as part of what became known as the ‘Developing Interactive Virtual Applications’ (DIVA) project. All course materials were provided on the storage device with a requirement for students to find and add new resources from their own research, which then had to be uploaded to a centrally shared resource bank. While the USB storage device as a ‘dumb’ device offered no access to the Internet or the course website, it could act as a bridge between contexts of use. Learning experiences in higher education typically involve the use of multiple technologies across a range of locations and contexts. Students quickly found the flexibility of the storage device invaluable, not only in storing found and newly developed resources of their own, but also in discussing their work with peers. Finding and sharing resources was a course requirement and formed part of summative assessment: analysis of usage of the storage device was recorded in a course log, resources were presented and discussed in seminars, and a snapshot of the content of each storage device revealed the extent of its use at the end of the course.

The main advantage of the storage device was that it was not seen as intruding in the learning process. The wide availability of access to IT for most students both on and off campus had diminished the value of continuous connectivity; the storage device, which is compatible with both Mac and Windows platforms, offered a ‘one stop shop’ for all the resources they required. For flexibility and sheer convenience, the USB storage device was preferred by students to the XDA. Most were reluctant to return it at the end of the term.

The technology

The USB storage device is a comparatively cheap technology costing approximately £41.00 according to storage capacity. To accommodate large files, devices of 256 MB were selected for the DIVA project. The storage devices are widely available and decreasing in price. They offer some advantages over floppy disks and CD-ROMs for moving files from place to place: they are less likely to be damaged in transit and, as they are supported effectively on both on Windows and Mac platforms, large files can be copied rapidly from computer to device. It is important to check if any USB ports within the institution, particularly in the learning resources area, are locked or inaccessible. Students using USB storage devices to carry important files between locations should make backup copies in case of loss. Unless devices are going to be given or sold on to students, conditions of return need to be clearly understood.

Students who are encouraged to take ownership of course resources become more confident learners and develop into more productive and innovative thinkers. The USB storage device offered an effective way of achieving this.

4.2. E-Learning Models

Generally speaking, E-Learning may be used to supplement either traditional contact education or print-based distance education or it may be a complete replacement of the traditional modes. Richards (2002) argues that "a distinction must be made between what may be referred to as an add-on model of E-Learning and a more integrated approach which goes beyond a mere transmission or delivery of content to promote more interactive and effective learning". It would be difficult to make this distinction, as E-Learning should be based on using the technology to support a good learning experience. A good learning experience is one in which a student can "...master new knowledge and skills, critically examine assumptions and beliefs, and engage in an invigorating, collaborative quest for wisdom and personal, holistic development" (Eastmond and Ziegahn, cited by Jonassen et al., 1995). The most valuable activity in a classroom of any kind is the opportunity for learners to work and interact together and to build and become part of a community of scholars and practitioners.

The E-Learning models have evolved from classroom replication towards models that integrate technology and pedagogical issues. While the first E-Learning models emphasised the role of the technology in providing content (information), delivery (access) and electronic services, more recent models focus on pedagogical issues such as online instructional design and the creation of online learning communities. Our ten selected, most popular and commonly used E-Learning models are sorted and compiled based on literature review, developers and vendors' (Blackboard, Bridge, PiiQ by Cornerstone, Docebo LMS, Saba logo, SAP SuccessFactors, eSSential LMS, Torch LMS, WorkWize LMS, Prosperity LMS, SkyPrep, SyberWorks, eLearning Cloud, Edvance360 Learning Management System, eCoach, Elan by Brainier, Schoox, CALF, Cornerstone OnDemand, Schoolwires and Moodlerooms) websites.

The models were reviewed and compared in order to understand the limitations of current Access Control and Copyright issues (see comparison analysis of the models in sub-section 4.2.11). The latter is well within our objective 4 (see sub-section 1.5. Research Aims and Objectives).

4.2.1. E-Learning Demand-driven Learning Model

The demand-driven learning model (see Figure 30) was developed in Canada as a collaborative effort between academics and experts from private and public industries (MacDonald et al., 2001). Although this model is based on the technology learning management system vendors' model of technology, content and service, the technology is seen as support or a tool to achieve the desired learning outcomes in a cost-effective way.

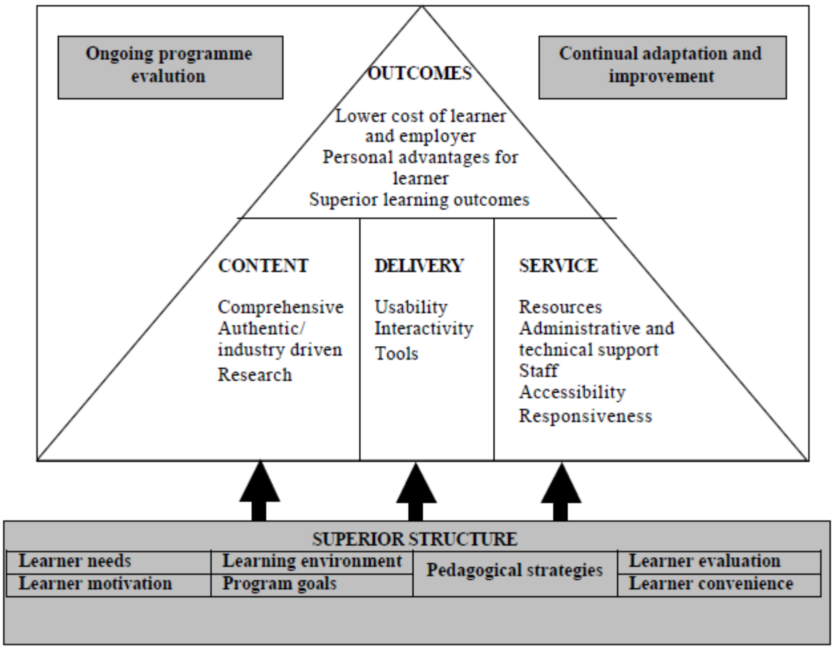


Figure 30. E-Learning Demand-driven Learning Model (MacDonald et al., 2001)

The primary purpose of the model is to encourage academics to take a proactive role in the development and use of technology in the teaching process. It emphasises the three consumer demands: high quality content, delivery and service. Content should be comprehensive, authentic and researched. Delivery is web-based, and the interface of E-Learning programmes should be user-friendly with communication tools to support interactivity. Service should include the provision of resources needed for learning as well as any administrative and technical support needed. As technology is fundamental to E-

Learning, this model provides a valuable framework for understanding the importance of investing in ICT infrastructure to support content, delivery and service. However, this model also highlights the importance of the needs of learners and their employers and the pedagogical changes that must be made to E-Learning content and services to meet these needs.

4.2.2. E-Learning Community of Inquiry Model

The community of inquiry model developed by Garrison and Anderson (2003) is an attempt to give educators an in-depth understanding of the characteristics of E-Learning and direction and guidance to facilitate critical discourse and higher-order learning through the use of E-Learning. A community of inquiry provides the environment in which learners can take responsibility for and control of their learning through interaction and is a requisite for higher-order learning. Given the information access and communication facilities of the Internet, an E-Learning system has distinct advantages as a mean of providing support to communities of inquiry to promote higher-order learning.

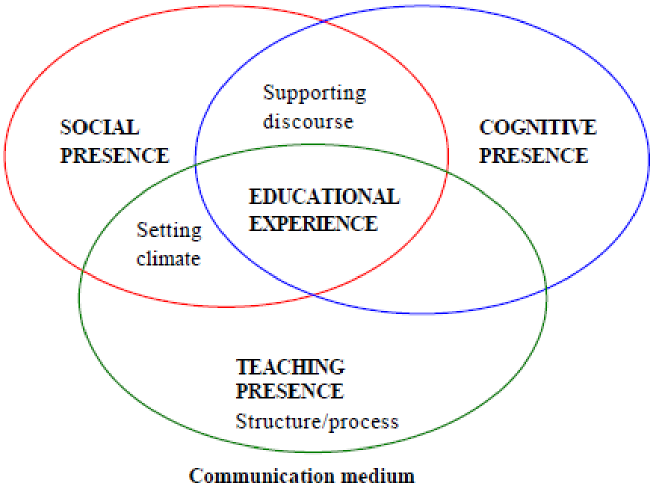


Figure 31. E-Learning Community of Inquiry Model (Garrison & Anderson, 2003)

The Community of Inquiry Model has three key elements that must be considered when planning and delivering an E-Learning experience (see Figure 31). They are cognitive presence, social presence and teaching presence:

- Cognitive presence
  The cognitive presence is the extent to which learners are able to construct and confirm meaning through sustained reflection and discourse in a critical community of inquiry. In essence, cognitive presence is a condition of higher-order thinking and learning.
- Social presence
  The Social presence defines the ability of participants in a community of inquiry to project themselves socially and emotionally, as 'real' people (i.e. their full personality), through the medium of communication being used.
- Teaching presence
  Teaching presence defines the design, facilitation and direction of cognitive and social processes for the purpose of realizing personally meaningful and educationally worthwhile learning outcomes.

The Community of Inquiry E-Learning Model is built on the demand-driven model and the instructional design models and draws attention to the complexities of communication in a virtual learning environment. Even in higher education today, the reality is that the concept of communities of inquiry that encourages learners to approach learning in a critical manner and process information in a deep and meaningful way has not been widely established. While this model may seem idealistic, the issue of interaction in the learning process has to be addressed.

4.2.3. Learning Objects Model

The Learning Object Model is based upon the notion of the 'learning object' as 'any digital resource that can be reused for to support learning' (Wiley, 2000; Fulantelli et al., 2008; Sinclair et al., 2013). However, learning objects have come to mean many things to many people (Polsani, 2003). Essentially the model has emerged from the potential of reusing learning materials and has been adopted as part of the development of standards for learning technology. Consequently, the model is rather more instructional and technological, to the extent that learning objects (LOs) have been described as 'an instructional technology' rather than a model or approach to learning per se (Wiley, 2000). Furthermore, the model is dependent upon the learning specifications and standards developed by the Learning Technology Standards Committee of the Institute of Electrical and Electronics Engineers set up in 1996. They define LOs as 'any entity, digital or non-digital, which can be used, re-used or referenced during technology supported learning' (IEEE LTSC definition cited in IMS Global Learning Consortium, 2002; Chikh, 2014).

Another positive strength of using learning objects is that it broadens the access that can be offered, as the object can be delivered digitally and over networks increasing the numbers and the limitless locations where objects can be reached. Extra functionality can be gained from recording the sequences of object use which may vary greatly according to context and place of use. Interoperability is another stated strength of the learning object model (LTSC, 2000; Mayes and de Freitas, 2004; Daniel et al., 2016).

The reusability of the objects and the broadened access provide the most compelling uses of objects. However, some weaknesses might include: changes to standards which might inhibit or restrict development, pedagogic neutrality of the objects, although this may not be a weakness but may allow tutors to develop their own pedagogic approaches to the material and the lack of contextual specificity, which in a context-specific learning environment may provide problems in terms of how the object is embedded. There is also an assumption that learning objects can be developed independently from tutors but can be generated by developers which would be problematic.

4.2.4. Laurillard Conversational Framework

The Laurillard Conversational Framework (2002) has been very influential in the development of UK E-Learning, at least among educational developers in High Education. Laurillard's analysis of academic learning as learning mediated through conversations between learners and teachers, rather than situated in direct experience, is the basis for describing five interdependent aspects of the academic learning process:

- The need to understand the structure of the academic discourse – organises and structures the content, through some kind of narrative
- Understand and practice the forms of representation
- Learn to manipulate these (acting on descriptions)
- Use feedback actively
- Learn to reflect on the goal-action-feedback cycle

Laurillard's description is based on constructivist's approach, but places more emphasis on the interaction between teacher and individual student, and stresses the need for meaningful intrinsic feedback to be a central feature of E-Learning. This sets out the requirements for academic learning, and how far current learning technology can help to meet the academic learning process by subjecting each ‘media form’ to an analysis in terms of the conversational framework is shown in Table 10.

Table 11. Mapping of learning experience onto Method, Technology and Media form

Learning experience	Methods/Technologies	Media forms
Attending, apprehending	Print, TV, video, DVD	Narrative
Investigating exploring	Library, CD, DVD, Web	Interactive
Discussion, debating	Seminar, online conference	Communicative
Experimenting, practising	Lab, field trip, simulation	Adaptive
Articulating, expressing	Essay, product, animation, model	Productive

(Laurillard, 2002)

4.2.5. Centre for Studies in Advanced Learning Technology (CSALT) Networked Learning Model

The Centre for Studies in Advanced Learning Technology (CSALT) at Lancaster University is one of Europe's leading academic research groups in the field of Technology Enhanced E-Learning (TEL) applied to adult education and training. The CSALT Networked Learning Model developed by Goodyear (2001) and his colleagues at Lancaster University is based firmly on both constructivist and CoP (Community of Practice) principles. The model is aimed particularly at tutors in higher education and includes a pedagogical framework as well as providing an overview of the broader issues surrounding networked learning. The pedagogical framework defined here introduces four levels of pedagogy: philosophy, high-level pedagogy, strategy and tactics. The upper two levels are considered as declarative or conceptual and the lower two levels are regarded as procedural or operational. The model (see Figure 32) suggests a distinction between the tasks designed by the tutor and the activities carried out by the learner. The networked learning model also integrates an element of the systems approach through a deeper analysis of the management by tutors of networked learning activities. The model is sensitive to organisational context and asserts its importance particularly in higher education settings.

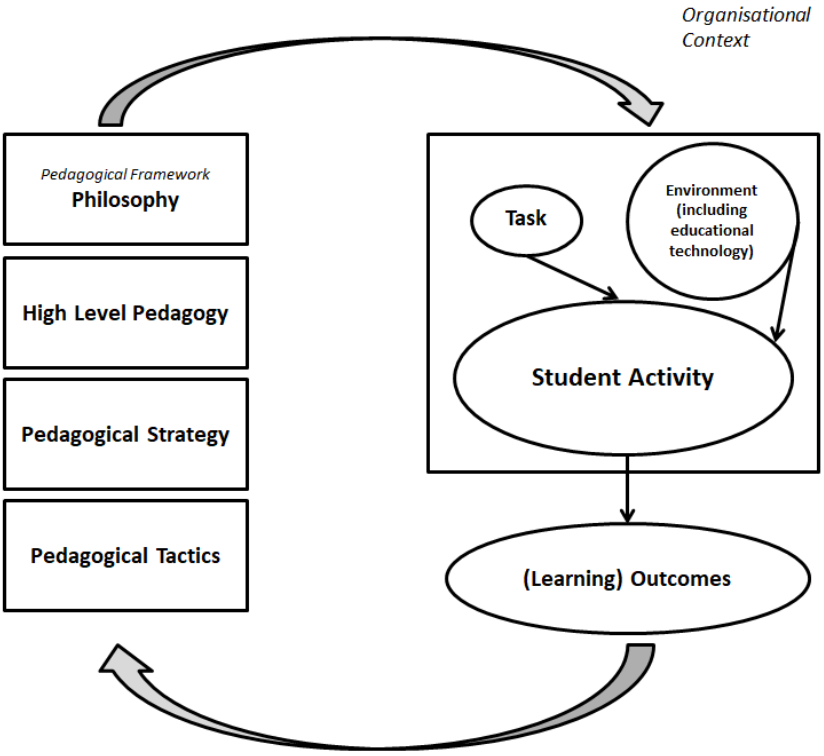


Figure 32. The CSALT Networked Learning Model (Goodyear, 2001)

This model provides a strong CoP perspective through the reification of knowledge about practice shared by the learners. The model is unusually strong in its focus on collaborative learning, taking the work of Dillenbourg (1999) as a basis for the analysis of online collaboration. Goodyear also emphasises the transformational and personal development aspects of networked learning. This model demonstrates how learning outcomes can be associated with specific supported learner groups and their activities need to be designed with these outcomes in mind.

4.2.6. Instructional Design Models for E-Learning

The Instructional Design Models for E-Learning based on the processes of designing, developing and delivering curriculum material are usually closely aligned with traditional classroom learning models that specify some combination of planning, implementing and evaluation to organise and present curriculum content. Instructional value is added by:

- customising content for the needs of the learners;
- presenting outcomes-based learning objectives;
- logically sequencing material to reinforce those objectives;

- basing navigational options (hypertext links) on existing and desired skills and knowledge of learners and
- designing objective-based, interactive learning activities that learners must complete to receive some form of evaluation.

Collis and Moonen (2001) identify institution, implementation, pedagogy and technology as the key components for developing online learning materials; Jolliffe et al. (2001) describe an 18-step process. Conrad's development model (2000) for an E-Learning experience has 7 stages comprising 21 tasks. Mishra (2001) identifies seven important factors when designing an online course. Alexander (2001) concludes that successful E-Learning takes place within a complex system involving the students' experience of learning, teachers' strategies, teachers' planning and thinking, and the teaching/learning context. However, they all emphasise the following issues:

1. Needs analysis that will investigate the following:
   - demand for instruction in the specific subject
   - demand and need for an online course
   - equivalence of an online course with face-to-face programmes
   - costs

2. Student profiles that will identify their needs and expectations, as follows:
   - age, gender, culture and work experience;
   - prior knowledge;
   - prior experience with E-Learning;
   - goals and motivation;
   - attitude towards E-Learning;
   - learning patterns and styles;
   - computer literacy;
   - access to computers and the Internet and
   - affordability of E-Learning.

3. Institutional support for E-Learning initiatives investigates the following:
   - the vision and mission of the institution;
   - lifelong learning as a goal of the institution;

- implementation costs and sustainability;
- experience of the lecturers and web designers;
- training for the lecturers;
- technological infrastructure and
- hardware and software and staff training in the systems and equipment.

4. Pedagogical choices that meet the requirements of the subject and the needs of the target learner group:

- learning models (constructivism versus behaviourism);
- learning objectives;
- delivery methods;
- assessment;
- interaction and
- development strategy: using individually available web tools (email, discussion groups and chat software) or an integrated course delivery software package such as WebCT or Blackboard.

The Instructional Design Models provide valuable frameworks for those responsible for developing E-Learning materials. These models are valuable for strategic planning, because they emphasise the issue of quality, quality of learning materials and quality of learning support.

4.2.7. Anderson and Elloumi's Model of Online Learning

Anderson and Elloumi's Model (2004) of online learning is a model that is focused on E-Learning with interactive triad – the interactive possibilities among students, teachers, and content.

The Anderson and Elloumi's Model of online learning illustrates the two major human actors, learners and teachers, and their interactions with each other and with content (see Figure 33). Learners can of course interact directly with content that they find in multiple formats, and especially on the Web; however, many choose to have their learning sequenced, directed, and evaluated with the assistance of a teacher.

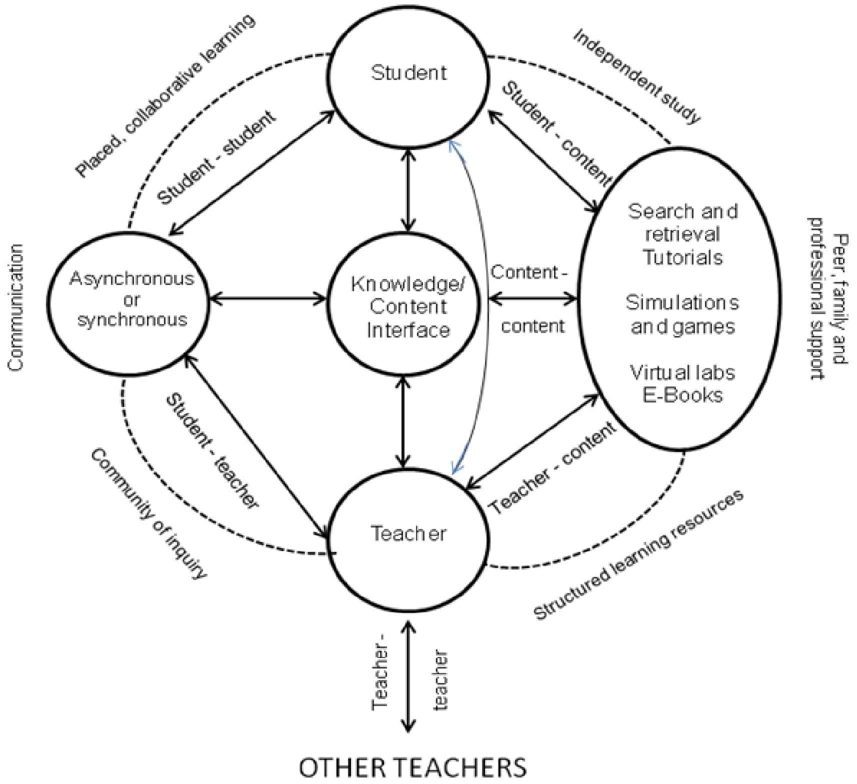


Figure 33. Anderson and Elloumi's Model of Online Learning
(Anderson and Elloumi's Model, 2004)

This interaction can take place within a community of inquiry, using a variety of Net-based synchronous and asynchronous activities (video, audio, computer conferencing, chats, or virtual world interaction).

4.2.8. Clark's Model of Instructional Systems Design

Clark's Model (2005) modifies the classic model of instructional systems design described by Dick and Carey. This model uses the familiar "ADDIE" design sequence (analysis, design, development, implementation, evaluation).

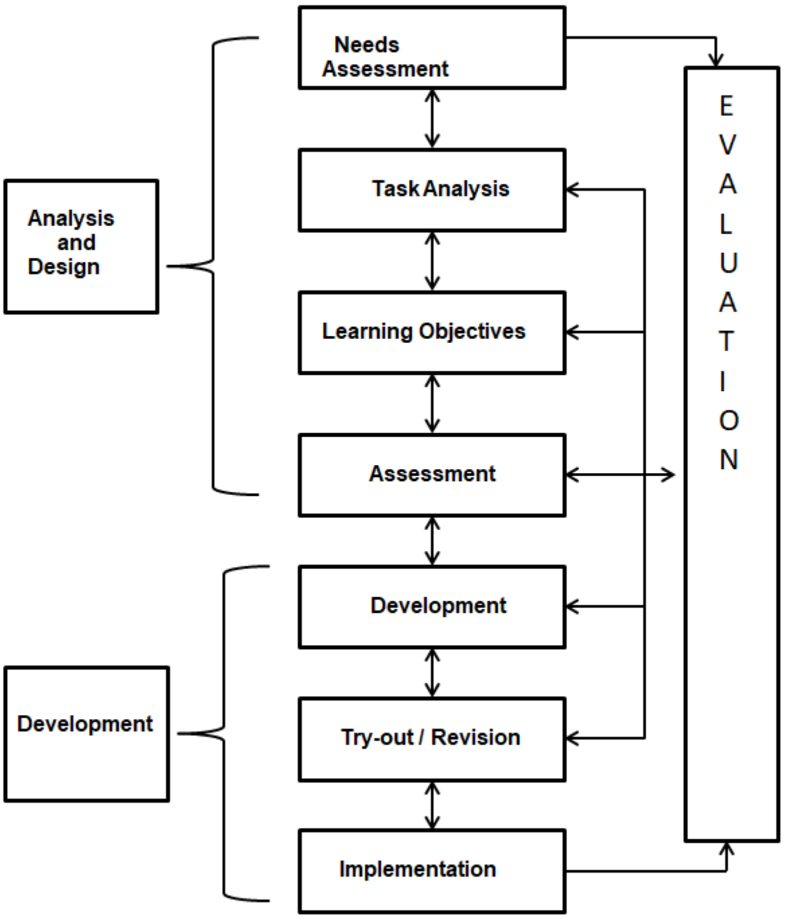


Figure 34. Clark's Model of Instructional Systems Design (Clark, 2005)

Clark updates this linear, industrial age view of instructional design by stressing the iterative and interactive nature of each step informed by frequent evaluations (see Figure 34).

4.2.9. Association for Educational Communications and Technology (AECT) Model of Instructional Technology

The Association for Educational Communications and Technology (AECT) model shows the five domains of competencies which are the foundations of the theory and practice of educational communication and instructional technology (Earle, 2000).

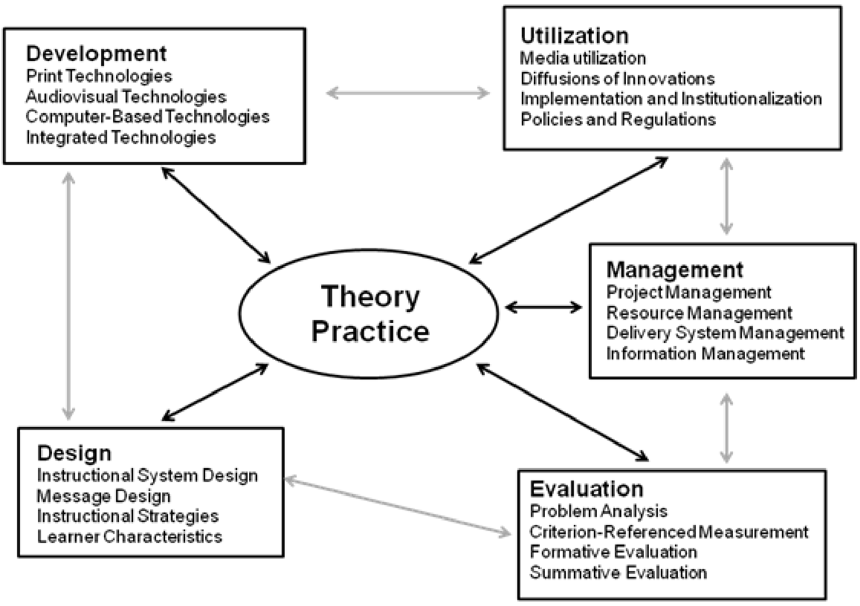


Figure 35. AECT's Model of Instructional Technology (Earle, 2000)

The five domains and the sub-domains in the AECT's model are proposed as an outline of professional competencies for instructional technology and design (see Figure 35).

4.2.10. International Society for Performance Improvement (ISPI) Model of Human Performance Technology

The International Society for Performance Improvement **(**ISPI) Model of Human Performance Technology is the latest version of the Human Performance Technology (HPT) model. The ISPI Model follows the five basic steps to improve human performance: a performance analysis, cause analysis, selection of intervention, design and development, implementation and evaluation (see Figure 36). The HPT is a multidisciplinary field of practice that has roots in the areas of instructional design, organizational and cognitive psychology and human resource development.

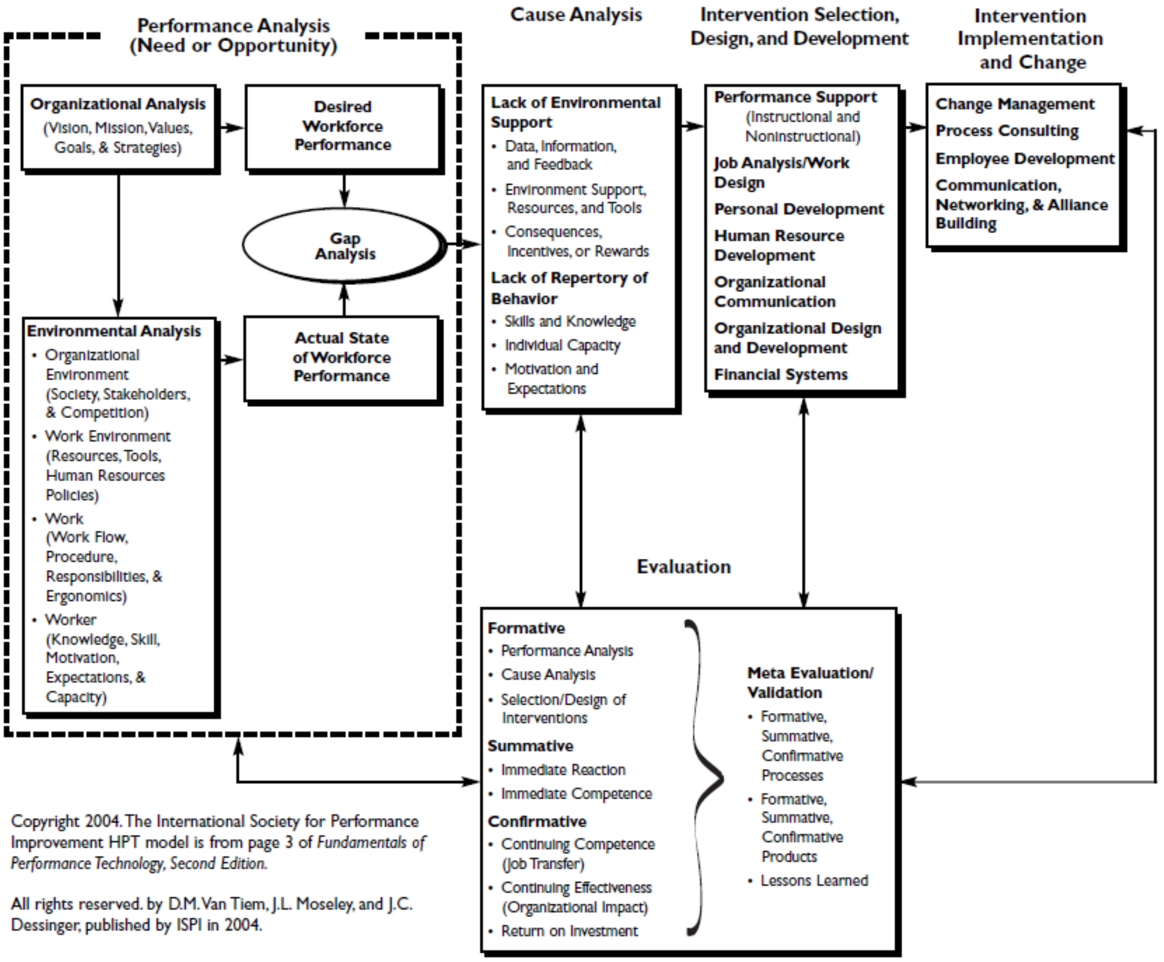

Performance Analysis
(Need or Opportunity)
Organizational Analysis
(Vision, Mission, Values, Goals, & Strategies)
Desired Workforce Performance
Gap Analysis
Environmental Analysis
• Organizational Environment (Society, Stakeholders, & Competition)
• Work Environment (Resources, Tools, Human Resources Policies)
• Work (Work Flow, Procedure, Responsibilities, & Ergonomics)
• Worker (Knowledge, Skill, Motivation, Expectations, & Capacity)
Actual State of Workforce Performance
Cause Analysis
Lack of Environmental Support
• Data, Information, and Feedback
• Environment Support, Resources, and Tools
• Consequences, Incentives, or Rewards
Lack of Repertory of Behavior
• Skills and Knowledge
• Individual Capacity
• Motivation and Expectations
Intervention Selection, Design, and Development
Performance Support (Instructional and Noninstructional)
Job Analysis/Work Design
Personal Development
Human Resource Development
Organizational Communication
Organizational Design and Development
Financial Systems
Intervention Implementation and Change
Change Management
Process Consulting
Employee Development
Communication, Networking, & Alliance Building
Evaluation
Formative
• Performance Analysis
• Cause Analysis
• Selection/Design of Interventions
Summative
• Immediate Reaction
• Immediate Competence
Confirmative
• Continuing Competence (Job Transfer)
• Continuing Effectiveness (Organizational Impact)
• Return on Investment
Meta Evaluation/ Validation
• Formative, Summative, Confirmative Processes
• Formative, Summative, Confirmative Products
• Lessons Learned

Figure 36. ISPI's Model of Human Performance Technology
(Sanders and Thiagarajan, 2001)

The HPT is based on the foundational belief that human performance can be improved using a systematic, systemic and results-based process (Sanders and Thiagarajan, 2001; Van Tiem, Moseley and Dessinger, 2012).

4.2.11. Comparative Analysis of Ten Existing E-Learning Models

The analysis of the ten existing E-Learning models that is tabulated in Table 12 shows that none of the models have builte-in security support. However, the only security that is being used is single-factor authentication based on username and password (log-in interface which is incorporated into the E-Learning system after the system has been developed – in-house security support).

Table 12. Comparative Analysis of the Ten Existing Models

Existing Models	Security Factors									Content delivery and assessment
	Access Control	Single-factor authentication	Two-factor authentication	Multi-factor Authentication	Security Policy	Copyright Policy	Biometrics	Device Enrolment	In-house security support	Focus on content delivery
1*	X	✓	X	X	X	X	X	X	✓	✓
2*	X	✓	X	X	X	X	X	X	✓	✓
3*	X	✓	X	X	X	X	X	X	✓	✓
4*	X	✓	X	X	X	X	X	X	✓	✓
5*	X	✓	X	X	X	X	X	X	✓	✓
6*	X	✓	X	X	X	X	X	X	✓	✓
7*	X	✓	X	X	X	X	X	X	✓	✓
8*	X	✓	X	X	X	X	X	X	✓	✓
9*	X	✓	X	X	X	X	X	X	✓	✓
10*	X	✓	X	X	X	X	X	X	✓	✓

Existing Models	
1* - E-Learning Demand-driven Learning Model	6* - Instructional Design Models for E-Learning
2* - E-Learning Community of Inquiry Model	7* - Anderson and Elloumi’s Model of Online Learning
3* - Learning Objects Model	8* - Clark's Model of Instructional Systems Design
4* - Laurillard Conversational Framework	9* - Association for Educational Communications and Technology (AECT) Model of Instructional Technology
5* - Centre for Studies in Advanced Learning Technology (CSALT) Networked Learning Model	10* - International Society for Performance Improvement (ISPI) Model of Human Performance Technology

It is worth noting that after using the above models to develop the E-Learning system, the only security that has been provided is the in-house security support, i.e. helping users to retrieve their usernames and passwords, or if there is any other problem in login to the system. The ten models mainly focus on content delivery and assessment. Therefore, security and Copyright are ongoing concerns for developers, content suppliers and users. Based on these findings we have integrated built-in security elements into the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

4.3. Summary of Chapter Four

This study has derived a wealth of data that may be used to understand how important security to E-Learning system. The analysis of six E-Learning case studies observations and comparing ten existing E-Learning models show that most E-Learning systems that are adopted by higher institutions/ or companies do not have E-Learning security model. Although there is support team at a distance that sometimes can be called upon to rescue minor issues, more often this support team might not be available at the time of needs. Considering the enormous costs involved in creating and maintaining courses, it is unfortunate that security is not yet considered as an important issue by many organisations. Unlike traditional security research, which has largely been driven by military requirements to enforce secrecy, in E-Learning it is not only the information itself that has to be protected but the way it is presented.

Based on the findings and outcomes of this Chapter, we have integrated the results into our proposed framework that will address how Access Control and Copyright can enhance security in E-Learning.

Chapter 5: Questionnaire Survey: Analysis of Security Issues in E-Learning

Introduction

A questionnaire survey was used to collect data on public opinion in relation to the security, attitude and awareness of E-Learning. The questionnaire was piloted, and we eliminated any inconclusive questions or questions that put potential respondents off, or questions that made the questionnaire time consuming to complete after gaining feedback. The questionnaire (see Appendix A: Security Issues in E-Learning Survey) has six sections:

- General information
- The impacts of E-Learning on the delivery of your programme(s)
- Risk assessment model for assessing the risk of E-Learning system
- Contents and Usage
- Security Measures
- Social Awareness

The questionnaire survey has 40 questions. In total 3370 questionnaire surveys were distributed via email and face-face to academic institutions and commercial sectors in the United Kingdom. Table 13 presents the questionnaire survey distribution frequency breakdown, which was segmented into three regions: Scotland, Wales and Northern Ireland and England (including London). This distribution coverage has enabled the geographical boundary of the UK to be covered. Among the total amount of distributed questionnaire surveys, we received 2970 incomplete questionnaires. The main target was to collect 400 completed questionnaires. The actual percent of response to each question is presented as “Valid Percent”. The column labeled "Valid Percent" is simply the proportion of a sample that is valid or the percentage of participants who completed and responded to all the questions in the questionnaire survey after eliminating the errors. We also presented “Cumulative Percent” in each Table. The “Cumulative Percent” column provided an easier way to compare different sets of data. The latter was another way of expressing frequency distribution.

The sample size of this research is based on the power analysis which suggests that conventions based on the premise with a large ratio of subjects will be reliable and closely estimate the true population values (Miller and Kunce, 1973). In order for us to have 100 completed questionnaires per region, we had to alter the questionnaire survey frequency by conducting a further survey using the same questionnaire (see Table 13). The sample of 400 was large enough for a research of this nature, given the time scale and the combination of research methods involved. The distribution of the questionnaire survey was conducted over a period of 18 months, between April, 2014 and June, 2015.

Table 13. Questionnaire survey distribution frequency

UK Regions	Questionnaire Survey Distribution Frequency	Incomplete Questionnaires (Errors)	Completed Questionnaires
Scotland	642	542	100
Wales and NI*	780	680	100
England (including London)	1948	1748	200
Total questionnaire surveys distribution	3370	2970	400

NI* (Northern Ireland)

The result generated data that was used to identify the security issues in E-Learning. It was possible to get this high feedback as a result of continuous friendly reminders via email and phone calls. The rationale for this purposive selection was to ensure that the questionnaire covers users, instructors and developers. This part of the research was to investigate the security threats to which E-Learning is exposed and how to assess the threats. There was also the issue of risk assessment. We hoped that the feedback would enhance the validity of the research results, and thus lend weight to the generalisation of the research findings and conclusions.

5.1. Section 1 of the Questionnaire Survey: General Information

Section 1 is based on the general Information consisting of seven separate questions. This section helps to give an overview of who generally uses E-Learning applications and if the respondents use E-Learning applications as part of their professional practice.

Question 1 is a closed question “Are you associated with a higher educational institution?” and it gives an overview of the amount of respondents who come from a higher educational institution. It is obvious that the highest amount of respondents to this question are from a higher institutions 92% (n=368) and only 8.0% (n=32) are from companies (see Table 14).

Table 14. Respondents from higher educational institutions

Question 1		Frequency	Percent	Valid Percent	Cumulative Percent
	No	32	8.0	8.0	8.0
	Yes	368	92.0	92.0	100.0
	Total	400	100.0	100.0	

Question 2 "Which of the following categories best describe your role in your institution / or company?" gives an overview of the job roles of all the respondents. It was very important to identify the respondents' professional roles within the institutions / or companies. Table 15 presents the job roles of all the respondents to the Question 2. The highest amount of respondents to this question are lecturers with 60.3% (n=241), followed by Post-Doc 12.3% (n=49). Post-Graduate students and Administrators represent the same share of respondents 9.3% (n=37).

Some of the respondents who participated in the survey are from British Telecom (BT), IBM, Microsoft and many other small and medium enterprises (SMEs), and this is reflected in the data. The reason for these companies' participation in the survey is that they are using E-Learning as for staff training. This reflection can be seen in Table 15 below with the percentage of managers at 5.5% (n=22) and technicians at 3.5% (n=14). The high respondents' rate from lecturers, Post-Doc, Post-Graduate students and administrators is expected, because most universities in UK have blended learning.

Table 15. Respondents' professional roles within the institutions / or companies

Job Categories	Frequency	Percent	Valid Percent	Cumulative Percent
Administrator	37	9.3	9.3	9.3
Lecturer	241	60.3	60.3	69.5
Manager	22	5.5	5.5	75.0
Post-Doc	49	12.3	12.3	87.3
Post Graduate	37	9.3	9.3	96.5
Technician	14	3.5	3.5	100.0
Total	400	100.0	100.0	

2.0% (n=8) of responses show that there are still some people who have not yet embraced E-Learning as the cultural norm of their institution or company.

Question 3 is a closed question "Do you use E-Learning as part of your teaching or professional practice?" and it shows the amount of respondents that use E-Learning as part of their teaching or professional practice. The results in Table 16 show that 98% (n=392) of respondents use E-Learning as part of their teaching or professional practice, while 2.0% (n=8) of respondents do not use E-Learning. The reason for the high percentage of users can be associated with the dramatical changes in how programmes and courses are delivered at the universities and to companies / or within companies to meet up with demand for those who cannot take time from work to go to full-time education.

Table 16. E-Learning as part of teaching or professional practice

E-Learning usage	Frequency	Percent	Valid Percent	Cumulative Percent
No	8	2.0	2.0	2.0
Yes	392	98.0	98.0	100.0
Total	400	100.0	100.0	

The results of this question are also supported by Gaebel et al. (2014): according to the survey that was conducted by the European University Association in 2013, 82% of institutions indicated that they offered online learning courses.

Question 4 reflects the significance of how important it is for people to realise their involvement or how they contribute to the development of E-Learning applications - “Do you develop E-Learning applications?”. Table 17 shows that only 14.0% (n=56) are involved in developing E-Learning applications, while 86.0% (n=344) are not involved in the process.

Table 17. Respondents’ involvement in developing E-Learning applications

	Frequency	Percent	Valid Percent	Cumulative Percent
No	344	86.0	86.0	86.0
Yes	56	14.0	14.0	100.0
Total	400	100.0	100.0	

The number of respondents that is involved in developing E-Learning applications cannot be underestimated, even though the percentage of those who are involved is very low.

Question 5 is specifically trying to find out the amount of respondents that is involved in training people on how to use E-Learning applications - “Do you train people on how to use the E-Learning applications?”. Table 18 shows that 81.0% of respondents are not involved in training people on how to use the E-Learning applications, while 19.0% of respondents do train people.

Table 18. Respondents' involvement in training people on how to use the E-Learning applications

	Frequency	Percent	Valid Percent	Cumulative Percent
No	324	81.0	81.0	81.0
Yes	76	19.0	19.0	100.0
Total	400	100.0	100.0	

The shortfall of our results in Table 18 can be attributed to the low amount of available trainers. As many institutions and companies are proclaiming the importance and cost benefit of E-Learning, there is still a massive gap on who can train the users. It can be argued that there are so many available manuals that users can follow step-by-step in accomplishing a particular circle of development. Nevertheless, the bulky part of the problem falls on the programmes and course developers who have to endure the pain on finding how to carry out certain tasks.

Question 6 "Are you a student in higher education?" shows the amount of respondents who are students that took part in the questionnaire. The findings show that 14.3% (n=57) of them are students (distance learners), 4.3% (n=17) are full-time students, 2.8% (n=11) are part-time students and 0.3% (n=1) are distance learners. The remaining 78.5% (n=314) who took part in the questionnaire are non-students (see Table 19).

Table 19. Response of students in higher education

	Frequency	Percent	Valid Percent	Cumulative Percent
Distance Learner	1	.3	.3	.3
No	314	78.5	78.5	78.8
Yes (Distance Learner)	57	14.3	14.3	93.0
Yes (Full-time student)	17	4.3	4.3	97.3
Yes (Part-time Student)	11	2.8	2.8	100.0
Total	400	100.0	100.0	

Question 7 "If you are a student, do you use E-Learning as part of your mode of learning?" is a follow-up of Question 6. The Table 20 shows that out of 86 students that took part in the questionnaire survey, 20.9% (n=18) of students, that took part in the survey, do use E-Learning as part of their mode of learning, while 79.1% (n=68) do not use it.

Table 20. Usage of E-Learning as part of the mode of learning by students

	Frequency	Percent	Valid Percent
No	68	79.1	79.1
Yes	18	20.9	20.9
Total	86	100.0	100.0

The results of this question can be supported by some of the researchers. As stated in the Canada21 report (Rogers at al., 2011) outlines critical issues faced by online components of university education, as many students reported negative opinions of E-Learning resources. It does not singularly address actual online teaching, but it still highlights likely resistance from those less comfortable with the online approach.

5.2. Section 2 of the Questionnaire Survey: The impacts of E-Learning on the delivery of your programme(s)

Section 2 focuses on the impacts of E-Learning on the delivery of respondents' programmes.

Question 8 "What type of learning approach has been adopted by your institution / or company?" gives an overview of learning approaches that were adopted by the respondents' institutions and companies. According to Table 21, 43.3% (n=173) indicated that their institutions/companies adopted Blended Learning (Classroom Leaning + Online Learning), 18.5% (n=74) - Blended Learning (Classroom Leaning + Mobile Learning), 25.5% (n=102) - E-Learning and 12.8% (n=51) - Training Courses.

Table 21. Adoption of learning approaches by institution/company

	Frequency	Percent	Valid Percent	Cumulative Percent
Blended Learning (Classroom Leaning + Online Learning)	173	43.3	43.3	43.3
Blended Learning (Classroom Leaning + Mobile Learning)	74	18.5	18.5	61.8
E-Learning	102	25.5	25.5	87.3
Training Courses	51	12.8	12.8	100.0
Total	400	100.0	100.0	

The results of Question 8 show that more and more institutions and companies combine online learning with traditional classroom methods. It is not surprising to see get these results. Miller (2017) stated that blended learning is more than just computer-based training; it is about leveraging technology to create a blend of different learning methods and modalities. Gupta (2016) also noted that blended learning is gaining school-wide support. She further emphasised that 59% teachers reported that students were more motivated to learn in a blended learning environment.

Question 9 "What types of technology do you use within your E-Learning system?" focuses on types of technology the respondents use within their E-Learning system. The findings show that 50.5% (n=202) respondents use Webinars. According to Christova and Mihai (2011), Webinars make knowledge and expertise more easily accessible, with geographical borders, disciplinary borders, but also the traditional teacher/student border becoming irrelevant within a common 'learning space'. It is not surprising that Webinars are widely used within the E-Learning system, as many users prefer having lectures or seminars that are transmitted over the Web using video conferencing software.

Table 22. Types of technology within E-Learning system

	Frequency	Percent	Valid Percent	Cumulative Percent
Data Conferencing	3	.8	.8	.8
E-mail	157	39.3	39.3	40.0
Mobile phone	17	4.3	4.3	44.3
Teleconferencing	5	1.3	1.3	45.5
Video Conferencing	4	1.0	1.0	46.5
Voice Mail	12	3.0	3.0	49.5
Webinars	202	50.5	50.5	100.0
Total	400	100.0	100.0	

The second highest feedback is email: 39.3% (n=157). Several studies also show that knowledge sharing via email is an effective E-Learning intervention (Alavi and Leidner, 2001; Renaud et al., 2006; Hwang, 2016). The rest of our feedbacks are on the lower side of 4.3% (n=17) Mobile phone, 3.0% (n=12) Voice Mail, 1.3% (n=5) Teleconferencing, 1.0% (n=4) Video Conferencing and 0.8% (n=3) use Data Conferencing (see Table 22).

Question 10 "From your experience, what are the impacts of E-Learning on your programme(s)/training?" presents the impacts of E-Learning on respondents' programmes/training. According to Figure 37, 26.3% (n=105) of respondents agree that E-Learning provides 24 hours a day 7 days a week availability, 25.8% (n=103) admit that E-Learning provides global accessibility from all over the world, 15.3% (n=61) agree with increasing speed with which teaching materials can be obtained, 11.8% (n=47) admit that

E-Learning provides reduced operations costs, 9.3% (n=37) agree that E-Learning promotes products to suit each individual learner, 7.5% (n=30) prefer increasing speed with which learning materials can be shared and 4.3% (n=17) agree that E-Learning provide access to search and retrieval systems.

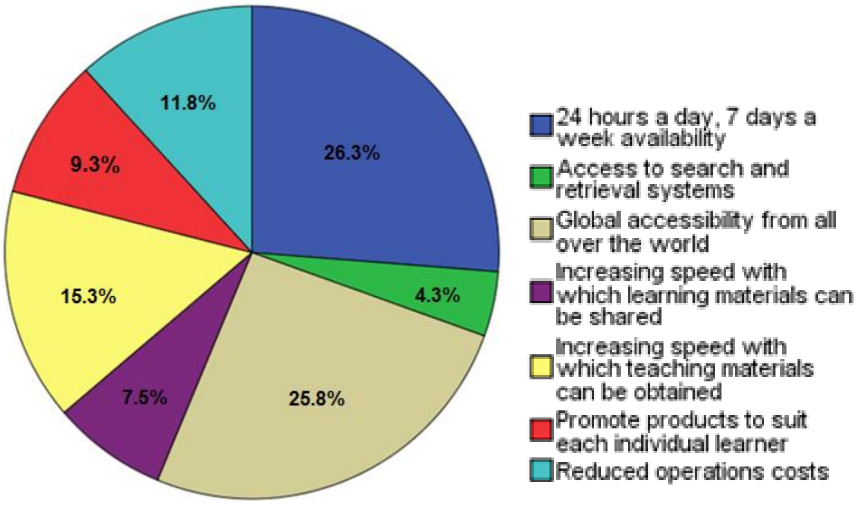


Figure 37. Impacts of E-Learning on Respondents' Programmes / Training

The results of Question 10 prove that users do like E-Learning within their programmes/training, as they can learn the subject at their own pace and in comfortable settings. If a learning tool is available 24/7, it is also beneficial for employers within the companies, as the employers can offer staff training without a constraint on resources.

Question 11 "What do you consider the top 3 reasons for not using the available E-Learning tools?" aims to identify the top 3 reasons for respondents not to use the available E-Learning tools. Out of 400 respondents, 76.0% (n=304) consider that security issues are one of the main reasons not to be using E-Learning tools, 9.8% (n=39) of respondents are inclined to lack of technical training, 7.5% (n=30) of respondents have chosen reliability on technology, 3.8% (n=15) - unfriendly or complicated learning system, 1.3% (n=5) - little or no focus on quality, 1.0% (n=4) - absence of the human touch, 0.8% (n=3) - lack of tutor support / readily available contact.

Based on the results that are outlined in Figure 38, the top 3 reasons for not using the available E-Learning tools can be identified as follows:

- Security issues;
- Lack of technical training;

- Reliability on technology.

It is not surprising that security issues have been identified by the respondents and it on the top of the list.

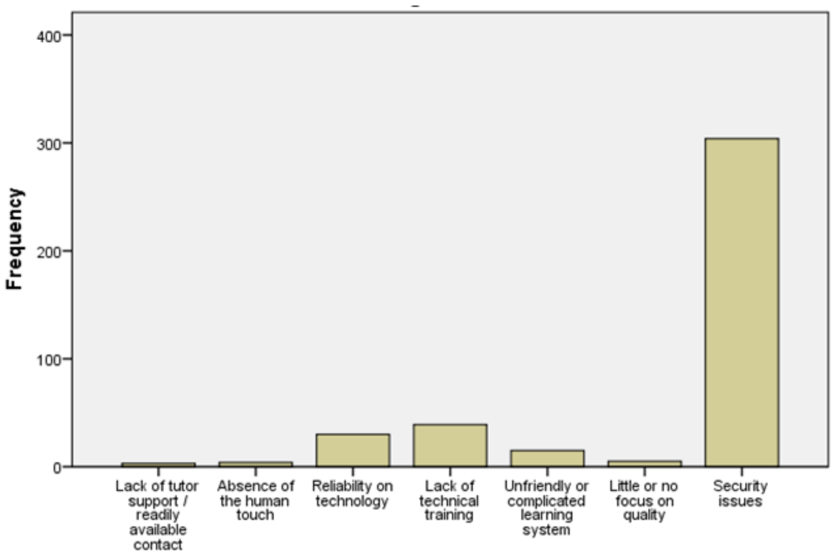


Figure 38. Top Reasons for not Using the Available E-Learning Tools

We further applied the cross-tabulation to Question 2 (“Which of the following categories best describe your role in your institution / or company?”) and Question 11 (“What do you consider the top 3 reasons for not using the available E-Learning tools?”).

Table 23. Cross-tabulation of Question 2 and Question 11

		What do you consider the top 3 reasons for not using the available E-Learning tools?							
		Lack of tutor support/readily available contact	Absence of the human touch	Reliability of technical training	Lack of technical training	Unfriendly or complicated learning system	Little or no focus on quality	Security issues	Total
Q2. Which of the following categories best describes your role in your institution?	Administrator	2.7%	2.7%	16.2%	10.8%		5.4%	62.2%	100.0%
	Lecturer	0.8%	0.8%	7.5%	8.3%	6.2%		76.3%	100.0%
	Manager			4.5%	9.1%		9.1%	77.3%	100.0%
	Postdoc			4.1%	14.3%			81.6%	100.0%

	Postgraduate		2.7%	5.4%	10.8%		2.7%	78.4%	100.0%
	Technician			7.1%	14.3%			78.4%	100.0%
Total		0.8%	1.0%	7.5%	9.8%	3.8%	1.3%	76.0%	100.0%

The results of our cross-tabulation for Questions 2 and 11 (see Table 23) show that Post-Doc students consider security issues the main reason for not using the available E-Learning Tools – 81.6% (n=40), followed by Technicians at 78.6% (n=11) and Post Graduate students at 78.4% (n=29). The above results show that there is high tendency for having more E-Learning users, if security aspects of E-Learning system can be enhanced by adopting the DEACCF.

5.3. Section 3 of the Questionnaire Survey: Risk Assessment Model for Assessing the Risk of E-Learning System

Section 3 focuses on the risks within E-Learning system. It also emphasises on risk assessment model in order to reveal the risks within E-Learning system.

Question 12 “As part of your role, do you identify critical risk exposures when using E-Learning applications or in the E-Learning system?” finds out if the respondents identify critical risk exposures when using E-Learning applications. And if so, how many of them identify critical risk exposures.

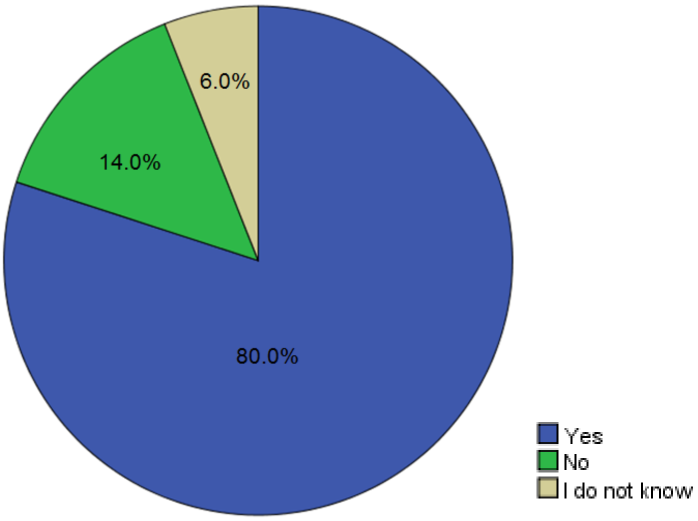


Figure 39. Critical Risk Exposures when Using E-Learning Applications

In Figure 39, 80.0% (n=320) of respondents identify critical risk exposures when using E-Learning applications, while 14.0% (n=56) of respondents do not and 6.0% (n=24) do not know. By applying cross-tabulations, we were able to find out the roles of respondents who identify critical risk exposures when using E-Learning applications (see Figure 40). The results show that out of 400 responses, 80% (n=320) stated that they do identify critical risk exposure. The highest respondents are lecturers at 47% (n=188), followed by Post-Doc students at 10.2% (n=41), administrators at 7.8% (n=31), Post-graduate students at 7.2% (n=29), and managers at 4.5% (n=18). The smallest group of respondents which identifies critical risk exposures while using E-Learning are technicians at 3.2% (n=13).

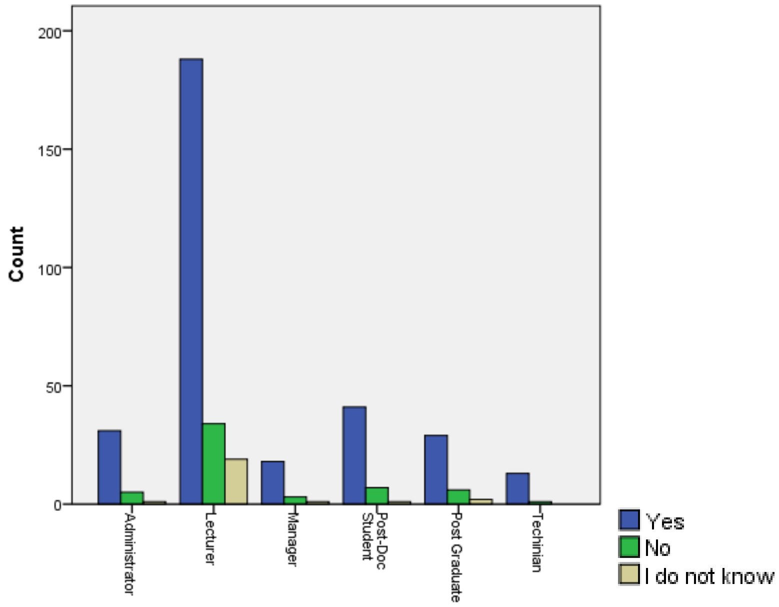


Figure 40. Respondents' Roles and Critical Risk Exposures when Using E-Learning Applications

The main reason for these staggering results is that lecturers intend to use E-Learning system on a daily basis than other categories of respondents.

Question 13 "Do you know if your institution /or company has a risk management policy in place?" shows us how many respondents are familiar with a risk management policy in their institutions/ or company. Figure 41 illustrates that 89.5% (n=358) of respondents do not know if their organisations have a risk management policy in place, 6.8% (n=27) – know that their organisations have risk management policy in place and 3.8% (n=15) of respondents know that their organisations do not have a risk management policy.

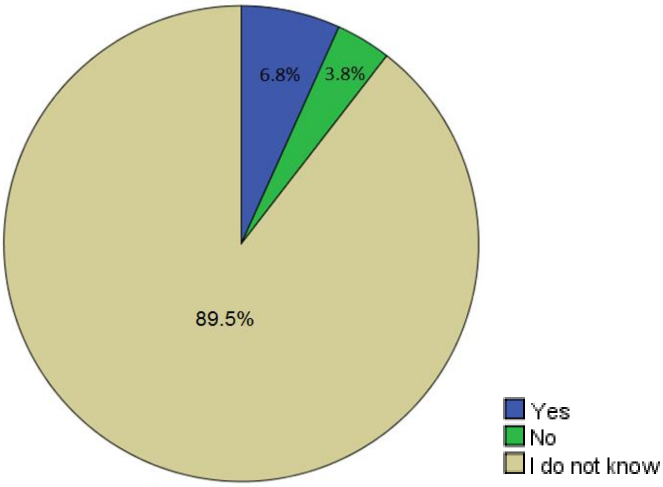


Figure 41. A Risk Management Policy within Institutions /or Companies

We further applied cross-tabulation to Question 2 ("Which of the following categories best describe your role in your institution / or company?") and Question 13 ("Do you know if your institution /or company has a risk management policy in place?"). The results show that 98.0% (n=48) of Post-Doc students, 97.3% (n=36) of Post Graduate students and 85.1% (n=205) of Lecturers do not know if their institution has a risk management policy in place. The results are very high for higher institutions. If users do not know if there is a risk management in place, they cannot trust E-Learning system.

Table 24. Cross-tabulation of Question 2 and Question 13

		Q13. Do you know if your institution /or company has a risk management policy in place?			
		Yes	No	I do not know	Total
Q2. Which of the following categories best describes your role in your institution?	Administrator	8.1%		91.9%	100.0%
	Lecturer	9.5%	5.4%	85.1%	100.0%
	Manager		4.5%	95.5%	100.0%
	Postdoc	2.0%		98.0%	100.0%
	Postgraduate		2.7%	97.3%	100.0%
	Technician			100.0%	100.0%
Total		6.8%	3.8%	89.5%	100.0%

Even though some companies are claiming that they are using E-Learning as part of their staff training, it is obvious that their staff are not familiar with the risk management policy. Our results show that 95.5% (n=21) of Managers do not know anything about it (see Table 24). The results of this question highlight that it will take longer than expected for E-Learning to be part of daily routine of programmes/or courses within any higher institution / or company.

Question 14 "Which of the following security risks is your institution /or company exposed to?" shows how well the respondents are familiar with security risks that their institution /or company is exposed to. The responses in Question 14 show that no application is 100% immune to security breaches. The results of the findings do not come as a surprise with all the publicity from both the news and research publications about E-Learning security risks. The feedbacks of security risks which the respondents are exposed to are detailed in Table 25.

Table 25. Types of security risks that institutions /or companies are exposed to

	Frequency	Percent	Valid Percent	Cumulative Percent
Malicious damage (e.g. corruption of data and software)	190	47.5	47.5	47.5
Unauthorised access (e.g. unauthorised viewing)	150	37.5	37.5	85.0
Accidental error/human carelessness (e.g. computer operator error)	15	3.8	3.8	88.8
Mechanical failure (e.g. hardware/software error damages file)	25	6.3	6.3	95.0
Invasion or loss of privacy/confidentiality	20	5.0	5.0	100.0
Total	400	100.0	100.0	

Table 25 shows that 47.5% (n=190) - pointed out malicious damage (e.g. corruption of data and software), 37.5% (n=150) of respondents chose unauthorised access (e.g. unauthorised viewing), 6.3% (n=25) - mechanical failure (e.g. hardware/software error damages file), 5.0% (n=20) - invasion or loss of privacy/confidentiality and 3.8% (n=15) identified accidental error/human carelessness (e.g. computer operator error). In support of the analysis of our findings, Benson and Brack (2010) and Versper et al. (2016) noted that an important administrative function in E-Learning was the completion of a risk assessment of four components: (1) student support factors (such as access and equity issues), (2) technical issues (such as access to hardware and software, bandwidth, etc.), (3) authentication (such as cheating, collusion, plagiarism, etc.) and (4) consideration of the instructor's administrative skills (such as ability to use software, manage online grading, copyright, etc.).

Question 15 "How do you assess the risks involved in using the E-Learning system?" - This question seeks the respondents' understanding and experiences of how they asses the risks involved in using the E-Learning system. The results in Figure 42 show that 3.8% (n=15) of respondents seek opinion of those already using the applications, 5.5% (n=22) - carefully analyse precedents to improve forecasting, 6.8% (n=27) - see the services of a risk consultant, 36.0% (n=144) - look at all of the things that could go wrong and develop a contingency plan in case they do.

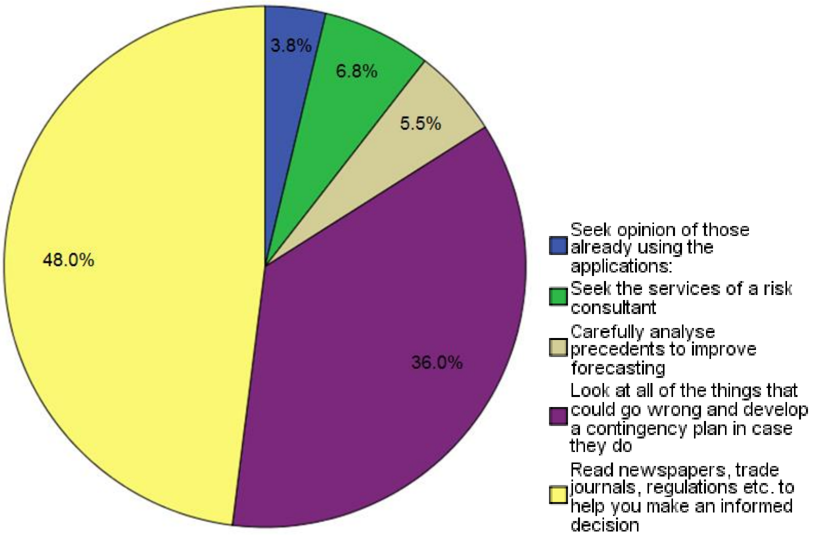


Figure 42. How Respondents Assess the Risks involved in Using the E-Learning System

Finally, 48.0% (n=192) of respondents read newspapers, trade journals, regulations etc. to help them make an informed decision. The survey results above show how respondents use a variety of ways to find information on how to assess the risks involved in using the E-Learning system.

Question 16 "Do you quantify risks in terms of their impact and probability?" shows how many respondents quantify risks in terms of their impact and probability. This was an expected feedback due to responses from questions 13. Table 26 presents the outcome of our findings - only 43.5% (n=174) of 400 responses quantify risks in terms of their impact and probability, 6.5% (n=26) do not quantify risks, while 50% (n=200) of respondents gave the answer “I do not know”.

Table 26. Quantifying Risks in terms of their Impact and Probability

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	174	43.5	43.5	43.5
No	26	6.5	6.5	50.0
I do not know	200	50.0	50.0	100.0
Total	400	100.0	100.0	

Schneier (2003) stated that “when we talk about risk, it is the likelihood of the threat and the seriousness of its successful attack. For example, a threat is more serious because it is more likely to occur”. The results of Question 16 show that majority of users do not know how to quantify risks in terms of the impact and probability, which proves that not much training is provided for E-Learning users.

Question 17 “Do you have a risk assessment / or management framework for your E-Learning applications?” aims to reveal if the respondents have a risk assessment / or management framework for your E-Learning applications. According to the results outlined in Table 27, 78.0% (n=312) of respondents do not have a risk assessment / or management framework for their E-Learning applications, 19.3% (n=77) - do not know and only 2.8% (n=11) do have a risk assessment / or management framework.

Table 27. A Risk Assessment / or Management Framework for E-Learning Applications

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	11	2.8	2.8	2.8
No	312	78.0	78.0	80.8
I do not know	77	19.3	19.3	100.0
Total	400	100.0	100.0	

We further applied cross-tabulation to Question 17 (“Do you have a risk assessment/ or management framework for your E-Learning applications?”) and Question 21 (“Do you consider your E-Learning system safe?”).

Table 28. Cross-tabulation of Question 17 and Question 21

		Q17. Do you have a risk assessment /or management framework for your E-Learning applications?			
		Yes	No	I do not know	Total
Q21. Do you consider your E-Learning system safe?	Yes		40.0%	60.0%	100.0%
	No	3.0%	78.2%	18.9%	100.0%
	I do not know		83.3%	16.7%	100.0%
Total		2.8%	78.0%	19.3%	100.0%

The results show that 78.2% (n=312) of respondents out of 400 stated that they do not have a risk assessment/ or management framework for their E-Learning applications and they do not consider their E-Learning system safe (see Table 28). The above results prove that most of E-Learning systems do not have risk assessment / or management framework. Therefore, system is prone to different breaches and attacks.

Question 18 "Are there any risk improvement measures in place?" is focused on risk improvement measures that respondents have in place. This question shows an extended outcome to the findings in questions 17 and 19. The Table 29 shows that 72.5% (n=290) gave "No" answer, which is very high; 25.8% (n=103) – do not know, and only 1.8% (n=7) answered "Yes".

Table 29. Risk Improvement Measures

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	7	1.8	1.8	1.8
No	290	72.5	72.5	74.3
I do not know	103	25.8	25.8	100.0
Total	400	100.0	100.0	

The outcomes of these results can be validated with Vesper et al. (2016) statement that "…even though the risk assessment is very useful in articulating potentially problematic events, such assessments are rarely performed in design and development of E-Learning systems even though significant risks may exist that may affect the implementation and ultimate effectiveness of the E-Learning".

Question 19 “Is there any system for identifying risks?” is trying to find out if there is any system for identifying risks. Out of 400 responses, 93.8 % (n=375) stated that there was no system for identifying risks, 4.5% (n=18) of respondents – do not know, and only 1.8% (n=7) admitted that there is a system for identifying risks (see Table 30).

Table 30. System of Identifying Risks

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	7	1.8	1.8	1.8
No	375	93.8	93.8	95.5
I do not know	18	4.5	4.5	100.0
Total	400	100.0	100.0	

There is significant correlation between responses to Question 19 and Question 31 (“Is your institution /or company's security and privacy policy available to the general public?”) of .106 at the 0.005 level (2-tailed). If the system is open to the general public, it means that the system will be vulnerable to risks and threats. Therefore, it is very important to have system for identifying risks. Based on these results there is an urgent need for risk improvement measures to be in place. For this reason, we have adopted CRAMM (Central Computing and Telecommunications Agency (CCTA) Risk Analysis and Management Method) to our proposed DEACCF, which is ISO/IEC 27001 compliant (see Chapter 5, sub-section 5.9.1).

Question 20 “Which of the following methods are used for managing the E-Learning risks within your institution /or company?” investigates which methods are used by respondents for managing the E-Learning risks within their institution /or company. According to Table 31, 77.0% (n=308) of respondents stated that their institution/ or company put safeguards and controls (e.g. policies, procedures etc.) in place, 7.0% (n=28) - use experienced and reliable dealers, 5.0% (n=20) - assess risk periodically, 4.5% (n=18) - agree a fixed fee with a risk management company, 3.3% (n=13) - take out an insurance policy, 2.5% (n=10) - absorb risk and only 0.8 (n=3) - forecast and plan ahead.

Table 31. Methods are used for Managing the E-Learning Risks within Institution /or Company

	Frequency	Percent	Valid Percent	Cumulative Percent
Take out an insurance policy	13	3.3	3.3	3.3
Absorb risk	10	2.5	2.5	5.8
Forecast and plan ahead	3	.8	.8	6.5

Agree a fixed fee with a risk management company	18	4.5	4.5	11.0
Use experienced and reliable dealers	28	7.0	7.0	18.0
Put safeguards and controls (e.g. policies, procedures etc.) in place	308	77.0	77.0	95.0
Assess risk periodically	20	5.0	5.0	100.0
Total	400	100.0	100.0	

An academic institution /or company that incorporates risk management into a management system can achieve better results and make more rational strategic decisions (Ruzic-Dimitrijevic and Dakic, 2014). The importance of risk management has been supported by Lessard and Lucea (2009) who stated that risk management can be the core competence of every business process and E-Learning system.

Question 21 “Do you consider your E-Learning system safe?” focuses on safety of E-Learning system. The results show that 92.8% (n=371) do not think that their E-Learning system is safe, 6.0% (n=24) of respondents do not know, and only 1.3% (n=5) do believe that their E-Learning system is safe (see Table 32).

Table 32. Safety of E-Learning System

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	5	1.3	1.3	1.3
No	371	92.8	92.8	94.0
I do not know	24	6.0	6.0	100.0
Total	400	100.0	100.0	

The results of Question 21 have significant correlation of .108 at the 0.05 level (2-tailed) with the results to Question 31 ("Is your institution /or company's security and privacy policy available to the general public?"). The results of Question 31 show that out of 400 respondents 84.3% (n=337) stated that their institution /or company’s security and privacy policy is not available to the general public. It means that institution /or company’s security and privacy policy either does not exist or is hidden. If the security and privacy policy is not in place, then E-Learning system cannot be considered safe. There is also a significant correlation of .101 at the 0.05 level (2-tailed) between the results of this question and Question 36 (“Which of the following risks do you think the E-Learning system is prone to?”).

If the E-Learning system is not safe, it is prone to different risks in relation to security breaches.

According to Alwi and Fan (2010), many educational institutions are rushing into adopting online learning management systems without careful planning and without a thorough understanding of the security aspects of E-Learning. As stated in Chapter 2 (sub-section 2.11.), E-Learning systems are vulnerable to several types of web attacks. Based on this fact, the respondents believe that the attackers can easily gain access to the E-Learning server. By doing so, they will get hold of users' credentials, which in many cases can have financial implications (ransomware attacks). Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid (Trend Micro, 2017). The outcomes of Question 21 clearly show that even though an academic institution / or company has policies or procedures in place, users do not consider E-Learning system safe.

Question 22 "Are remote users authenticated before being allowed to connect to internal networks and systems?" investigates if remote users are authenticated before being allowed to connect to internal networks and systems. The Figure 43 shows that 23.8% (n=95) of respondents admitted that remote users are authenticated before being allowed to connect to internal networks and systems, while 28.8% (n=115) do not know. The overwhelming 47.5% (n=190) of respondents stated that remote users are not authenticated at all.

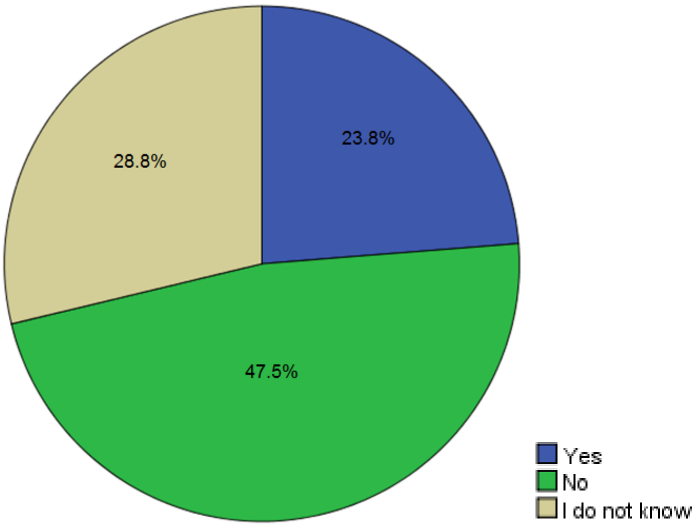


Figure 43. Remote Users' Authentication

We further applied cross-tabulation to Question 22 (“Are remote users authenticated before being allowed to connect to internal networks and systems?”) and Question 34 (“Are you required to use any other authentication method apart from the password?”). The results show that 46.7% (n=155) of respondents stated that remote users are neither authenticated before being allowed to connect to internal networks and systems, nor they are required to use any other authentication method apart from the password (see Table 33).

Table 33. Cross-tabulation of Question 22 and Question 34

		Q22. Are remote users authenticated before being allowed to connect to internal networks and systems?			
		Yes	No	I do not know	Total
Q34. Are you required to use any other authentication method apart from the password?	Yes	25.0%	51.5%	23.5%	100.0%
	No	23.5%	46.7%	29.8%	100.0%
Total		23.8%	47.5%	28.7%	100.0%

The outcomes of these results show that remote users are not authenticated with multi-factor authentication method. Therefore, it shows that multi-factor authentication needs to be implemented to E-Learning system to make it more robust to withstand any external intrusion or threat.

5.4. Section 4 of the Questionnaire Survey: Contents and Usage

Section 4 is focused on contents and usage of E-Learning applications within respondents’ institutions / companies.

Question 23 “What is the proportion of the overall content of your module that is available on the course website?” gives an overview of the content that is available on the respondents’ website.

Table 34. Proportion of the Overall Content that is available on the Course Website

Proportion of the overall content	Frequency	Percent	Valid Percent	Cumulative Percent
100%	143	35.8	35.8	35.8
75%	220	55.0	55.0	90.8
50%	16	4.0	4.0	94.8
25%	21	5.3	5.3	100.0
Total	400	100.0	100.0	

According to Table 34, 35.8% (n=143) stated that all 100% of module's content is available on the course website, while 55% (n=220) of respondents claim that only 75% of content is available, 4.0% (n=16) stated that only 50% of content is available and 5.3% (n=21) have access only to 25% of the overall content of their module. Question 23 results show that many users, 55% (n=220), are able to access the content of the course website 24/7. On the other hand, the system becomes prone to different attacks, if there is no proper Access Control in place that can deter the intrusion. This is why we proposed the multi-factor authentication in our framework.

Question 24 "How often do you access the course materials?" shows how often the respondents access the course materials. According to Table 35, only 3.5% (n=14) access the course materials daily, 6.5% (n=26) do access the course materials once a week, 23.5% (n=94) – twice a week, and overwhelming 66.5% (n=266) of respondents access their course materials once a month.

Table 35. Frequency of Accessing the Course Materials

	Frequency	Percent	Valid Percent	Cumulative Percent
Daily	14	3.5	3.5	3.5
Once a week	26	6.5	6.5	10.0
Twice a week	94	23.5	23.5	33.5
Once a month	266	66.5	66.5	100.0
Total	400	100.0	100.0	

Even though the results of Question 23 showed that large number of users indicated that 75% of of the overall content is available on the course website, the results of Question 24 revealed that very small number of users, 3.5% (n=14), are accessing the course materials on a daily basis, compared to 66.5% (n=266) users who are accessing it once a month. We further applied cross-tabulation to Question 24 ("How often do you access the course materials?") and Question 34 ("Are you required to use any other authentication method apart from the password?”). The results show that 92.9% (n= 13) of respondents access the course materials daily and they are not required to use any other authentication method apart from the password (see Table 36). Only 7.1% (n=1) accesses his/her course materials on a daily basis and is asked to use any other authentication method apart from the password.

Table 36. Cross-tabulation of Question 24 and Question 34

		Q24. How often do you access the course materials?				
		Daily	Once a week	Twice a week	Once a month	Total
Q34. Are you required to use any other authentication method apart from the password?	Yes	1.5%	5.9%	17.7%	77.9%	100.0%
	No	3.9%	6.6%	25.3%	64.2%	100.0%
Total		3.5%	6.5%	23.5%	66.5%	100.0%

The above results show that majority of institutions/ or companies still have only single-factor authentication method within E-Learning system. The lack of strong authentication method in E-Learning system can also explain the number of users who access their course materials once a month - 80.1% (n=213) of users access the course materials once a month and they are not required to use any other authentication method apart from the password.

Question 25 “How would you rate the ease of using the E-Learning system in your institution /or company?” shows us how easy the respondents find the use of E-Learning system.

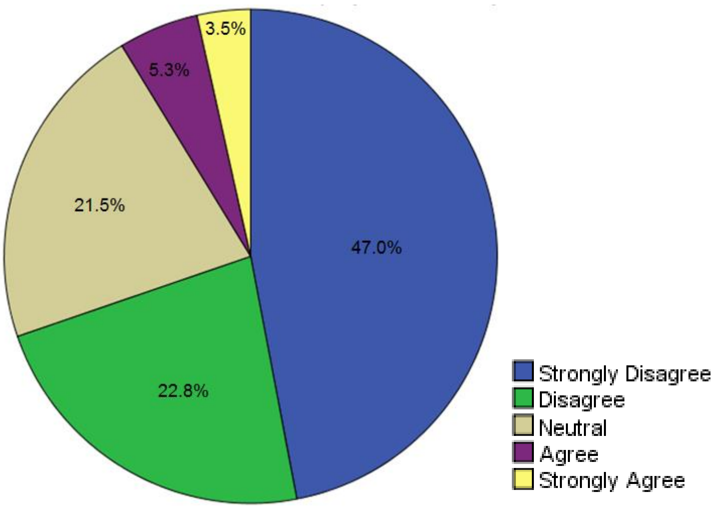


Figure 44. The Ease of Using the E-Learning System

Figure 44 shows that only 3.5% (n=14) of respondents strongly agree that is easy to use the E-Learning system in their institution /or company, which is very low. 5.3% (n=21) of respondents agree, 21.5% (n=86) – are neutral, 22.8% (n=91) of respondents disagree, and 47.0% (n=188) of respondent strongly disagree and they do not find it easy to use the E-Learning system in their institution / or company.

Question 26 "What is your experience of using the following tools in your E-Learning system?" is focused on respondents' experience of using the tools in their E-Learning system.

Table 37. The Respondents' Experience of Using the tools in their E-Learning System

Tools	Very Useful	Useful	Not useful	Do not know	Cannot remember
a. Discussion	29.8%(n=119)	14.3(n=57)	52.3%(n=209)	3.3%(n=13)	0.5%(n=2)
b. Lecture slides	25.5%(n=102)	6.8%(n=27)	65.5%(n=262)	1.8%(n=7)	0.5%(n=2)
c. Lecture notes	22.3%(n=89)	3.5%(n=14)	69.3%(n=277)	4.3%(n17)	0.8%(n=3)
d. Past question paper	16.8%(n=67)	12.3%(n=49)	45.5%(n=182)	18.0%(n=72)	7.5%(n=30)
e. Class experiment	22.0%(n=88)	15.3%(n=61)	54.0%(n=216)	3.8%(n=15)	5.0%(n=20)
f. Timetable	12.3%(n=49)	27.8%(n=111)	56.0%(n=224)	2.5%(n=10)	1.5%(n=6)
g. Self-assessment	4.8%(n=19)	9.3%(n=37)	76.8%(n=307)	7.5%(n=30)	1.8%(n=7)
h. Interactive lectures	12.5%(n=50)	21.5%(n=86)	64.3%(n=257)	1.3%(n=5)	0.5%(n=2)
i. News and alerts	3.3%(n=13)	5.3%(n=21)	90.8%(n=363)	0.5%(n=2)	0.3%(n=1)
j. Announcements	2.8%(n=11)	6.0%(n=24)	88.8%(n=355)	1.8%(n=7)	0.8%(n=3)
l. Charts	8.3%(n=33)	12.8%(n=51)	66.0%(n=264)	9.5%(n=38)	3.5%(n=14)
m. Who's online	16.0%(n=64)	10.8%(n=43)	59.5%(n=238)	11.3%(n=45)	2.5%(n=10)

According to the results that are outlined in Table 37, the highest number of respondents consider "Discussion" very useful - 29.8% (n=119), whereby only 2.8% (n=11) of respondents consider "Announcements" very useful. We were expecting that the latter will have the highest number of respondents, because this is the lifeline of communication within E-Learning system.

Question 27 “Do you trust that resources available online (lecture notes, tutorials, workshops, etc.) are a good substitute for the actual classroom learning?” focuses on the respondents’ trust in online resources. According to Figure 45, only 2.5% (n=10) of respondents trust that resources available online are a good substitute for the actual classroom learning and overwhelming 97.5% (n=390) do not trust online resources.

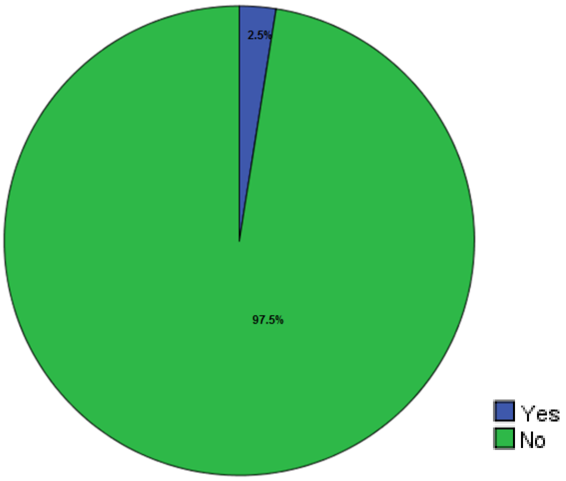


Figure 45. The Respondents’ Trust in Online Resources

The results of this question and Question 11 (“What do you consider the top 3 reasons for not using the available E-Learning tools?”) have a significant correlation of .101 at the 0.05 level (2-tailed). The outcomes of Question 11 show that out of 400 respondents 76.0% (n=304) consider that security issues are one of the main reasons not to be using E-Learning tools, while the outcomes of Question 27 show that an overwhelming 97.5% (n=390) number of respondents do not trust online resources. Therefore, users do not trust resources available online (lecture notes, tutorials, workshops, etc.) or E-Learning tools due to the lack of security measures. Our proposed DEACCF will enhance security measures and give users confidence and restore trust in E-Learning system.

5.5. Section 5 of the Questionnaire Survey: Security Measures

Section 5 of the questionnaire survey focuses on security measures in E-Learning system.

Question 28 “In your opinion is E-Learning security an important issue for your institution /or company?” draws more attention to the importance of E-Learning security in institutions and companies. The analysis of the question shows that 95.3% of respondents consider E-Learning security an important issue. The collective "Yes" responses are from institutions (75.3%) and companies (20%). Based on the "No" responses, 1.3% are from institutions and 1 valid percent from companies, while the "Unsure" responses are 1.3% from institutions and 1.2% from companies.

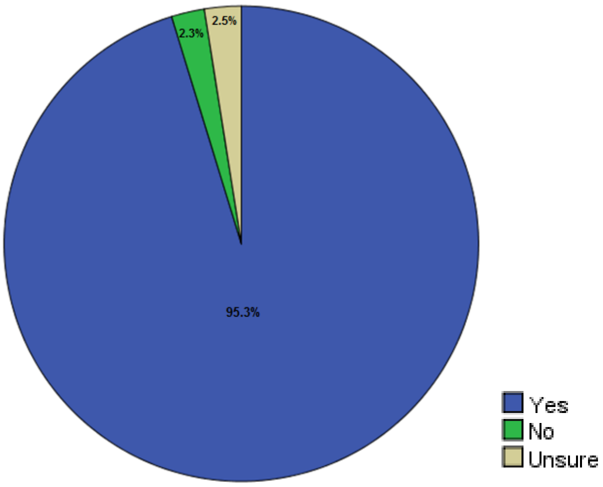


Figure 46. The importance of E-Learning Security in Institutions / or Companies

Figure 46 presents the perceived magnitude of impacts of security issues in E-Learning within institutions and companies. Without doubt, users are concerned about E-Learning security within their organisations. The results of our findings can be supported by the study that was presented by CSO Magazine (2011) which revealed that security attacks are a reality for most organizations: 81% of respondents' organisations experienced a security event (i.e. an adverse event that threatens some aspect of security).

Question 29 “Do you know that the learning system adopted by your institution is Internet based and can be prone to intrusion by attackers?” shows how the respondents are familiar with the learning system in their institutions/ or companies with regards to intrusions by attackers. The results are outlined in Table 38.

Table 38. The Proneness of the Learning System to Intrusion by Attackers

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	395	98.8	98.8	98.8
No	5	1.3	1.3	100.0
Total	400	100.0	100.0	

It is quite surprising that only 1.3% (n=5) of respondents do not know that that the learning system adopted by their institution is Internet based and can be prone to intrusion by attackers. The majority of respondents, 98.8% (N=395) do now about it. Today broadband and Internet access are very critical for institutions and companies. Without Internet, users will not be able to access their programme /or course. Any system that is exposed to the Internet is vulnerable to attacks which are increasing in terms of both numbers and complexity. It is not surprising that the majority of our respondents are aware of this fact.

Question 30 "Do you know if security policy in relation to E-Learning has been implemented in your institution / or company?" investigates if a security policy has been implemented in respondents' institutions / or companies in relation to E-Learning. The results are outlined in Figure 47. The analysis of the question shows that only 21.8% (n=87) do know that security policy in relation to E-Learning has been implemented in their institutions / or companies and an overwhelming 59.3% (n=237) do not know anything about it. Out of 400 respondents, 19.0% (n=76) of respondents are not sure.

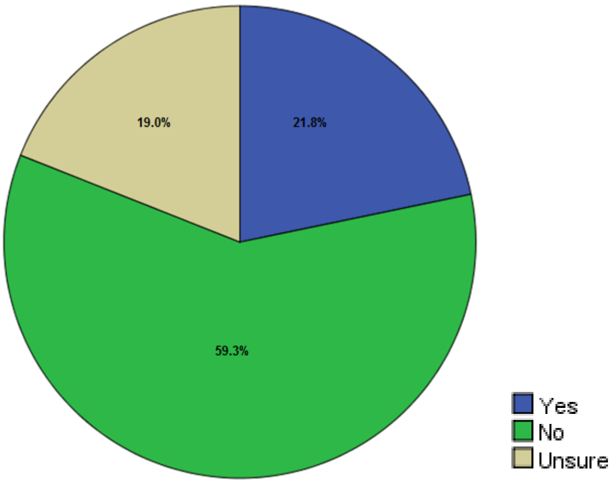


Figure 47. The Implementation of Security Policy in relation to E-Learning in the Respondents' Institutions/ or Companies

The results of this question are not surprising and can be associated with the results of Question 17, which shows that 78.0% (n=312) of respondents do not have a risk assessment / or management framework for their E-Learning applications. Furthermore, there is significant correlation of .101 at the 0.05 level (2-tailed) between Question 28 "In your opinion is E-Learning security an important issue for your institution /or company" and Question 30. Even though users are aware of the importance of E-Learning security, institutions /or companies do not make any effort to create an awareness or publicise the security policies. Miločević (2013) stated that a significant number of E-Learning platforms do not even have a basic policy defined at all. Less than half of E-Learners read the usage policy that is implemented by academic institutions / or companies (Miločević et al., 2016). The results of Question 30 show that users are not aware of E-Learning security policy in their institutions/ or companies, which prove that E-Learning security policy either has not been implemented, or it has been hidden from users.

Question 31 "Is your institution /or company's security and privacy policy available to the general public?" shows if security and privacy policy within the respondents' institutions /or companies are available to the general public.

Table 39. The Availability of Institutions /or Companies' Security and Privacy Policy to the General Public

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	15	3.8	3.8	3.8
No	337	84.3	84.3	88.0
Unsure	48	12.0	12.0	100.0

The results show that out of 400 respondents 84.3% (n=337) gave "No" response, while only 3.8% (n=15) answered "Yes", 12.0% (n=48) of respondents gave "Unsure" response (see Table 39). The security and privacy policies should be transparent in order to build user's confidence and trust.

Question 32 "Which of the following measures is required for login?" reveal a mixed picture in respect of what type of authentication methods are in place within the respondents' E-Learning systems. Accordingly, the survey results in Table 40 revealed that password has the highest responses at 83.3% (n=333), followed by biometrics at 7% (n=28). The results also show that 4.3% (n=17) of respondents choose public key encryption, 3% (n=12) are inclined for firewall and 1.8% (n=7) support private key encryption. The responses to the digital signature seems to be very low at 0.8% (n=3). Surprisingly, a digital signature is one of the requirements for submitting online student coursework and for validating students' visits to certain E-Learning modules /or programmes. However, most institutions and companies have not yet implemented the digital signature in their E-Learning system. Some of the reasons for this are that the current E-Learning applications in use need updates, the cost of updates - including licensing - is very high, and compatibility issues with their legacy systems.

Table 40. The required Measures for Login

	Frequency	Percent	Valid Percent	Cumulative Percent
Password	333	83.3	83.3	83.3
Firewall	12	3.0	3.0	86.3
Public Key Encryption	17	4.3	4.3	90.5
Private Key Encryption	7	1.8	1.8	92.3
Digital Signature	3	.8	.8	93.0
Biometrics	28	7.0	7.0	100.0
Total	400	100.0	100.0	

The results of Question 39 show that most institutions/ or companies are using single-factor authentication, as password has the highest responses at 83.3% (n=333). Furthermore, there is significant correlation of .208 at the 0.01 level (2-tailed) between the results of Question 32 and Question 33 (“Do you share your login details with anyone?”). If the system has only single- or two-factor authentication methods, it is quite easy to share the login details with someone else. However, if the system has a multi-factor authentication method, it will be quite difficult to share the login details. The lack of strong authentication in E-Learning can lead to various security threats and breaches, which were discussed in Chapter 2 (sub-section 2.8.6.). For this reason, we proposed the multi-factor authentication method and incorporated the E-Learning Security Threats Risk Assessment Model based on hybrid approach that will enhance the security of the Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

Question 33 “Do you share your login details with anyone?“ show how often the respondents share their login details with anyone. According to the results outlined in Table 41, only 1.3% (n=5) never share their login details, 7.5% (n=30) do it rarely, 37.5% (n=150) share their login details sometimes, 47.8% (n=191) usually share their login details and 6.0% (n=24) do share their login details every time.

Table 41. Sharing the Login Details

	Frequency	Percent	Valid Percent	Cumulative Percent
Never	5	1.3	1.3	1.3
Rarely	30	7.5	7.5	8.8
Sometimes	150	37.5	37.5	46.3
Usually	191	47.8	47.8	94.0
Every time	24	6.0	6.0	100.0
Total	400	100.0	100.0	

It is very surprising that the majority of respondents share their login details (“Usually” – 47.8% (n=191) and “Sometimes” – 37.5% (n=150), as most of the respondents acknowledged that the learning system adopted by their institution is Internet based and can be prone to intrusion by attackers in Question 29. The fact that a large amount of respondents share the login details proves that respondents are not familiar with institution/or company security policy and it has been justified in Question 30. Furthermore, Question 33 and Question 34 (“Are you required to use any other authentication method apart from the password?”) have significant correlation of .128 at the 0.05 level (2-tailed). Majority of respondents share their login details with someone else, as there is no other authentication method apart from the password. If the system has multi-factor authentication method which requires biometrics, it will be difficult and sometimes impossible to share the login details with someone else, unless the person is under duress.

Question 34 “Are you required to use any other authentication method apart from the password?” shows if the respondents are required to use any other authentication method apart from the password.

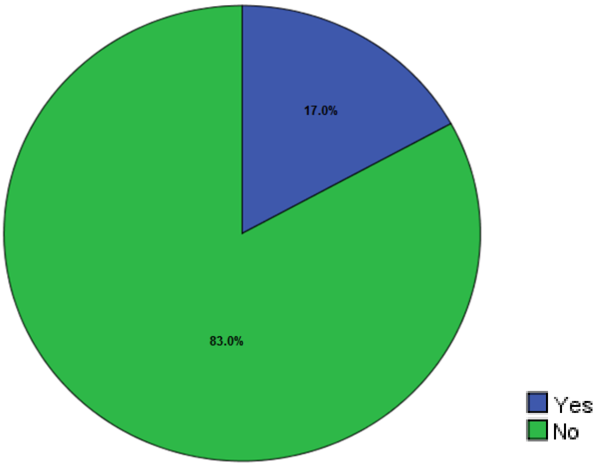


Figure 48. The Usage of any other Authentication Method apart from the Password

According to Figure 48, only 17.0% (n=68) of respondents are required to use any other authentication method apart from the password and the overwhelming 83.0% (n=332) – are not. It is quite surprising to see that majority of higher institutions and companies do not have any other authentication method apart from the password. Having only one authentication method shows how vulnerable E-Learning system can be. The results of this question justify the results of Question 7 why not many students use E-Learning as part of their mode of learning. Furthermore, we have applied cross-tabulation to Question 21 (“Do you consider E-Learning system safe?”) and Question 34 (“Are you required to use any other authentication method apart from the password?”).

Table 42. Cross-tabulation of Question 21 and Question 34

		Q34. Are you required to use any other authentication method apart from the password?		
		Yes	No	Total
Q21. Do you consider your E-Learning system safe?	Yes		100.0%	100.0%
	No	17.8%	82.2%	100.0%
	I do not know	8.3%	91.7%	100.0%
Total		17.0%	83.0%	100.0%

The analysis of our results shows that 91.0% (n=305) of respondents are not required to use any other authentication method apart from the password and they do not consider their E-Learning system safe, while 0% (n=0) of respondents are required to use other authentication method and consider their E-Learning system safe (see Table 42). Based on the latter, we introduce multi-factor authentication in our proposed DEACCF (see Chapter 6).

Question 35 “Are you able to access resources /or services off-campus?” shows how many respondents are able to access resources /or services off-campus. According to the results outlined in Figure 49, only 26.3% (n=105) of respondents are able to access resources /or services off-campus, but 73.8% (n=295) are not able to do so. There is significant correlation of .101 at the 0.05 level (2-tailed) between the results of Question 35 and Question 36 "Which of the following risks do you think the E-Learning system is prone to?". If a user is able to access resources /or services off-campus and there is no proper authentication system in place, it is obvious that the E-Learning system will be prone to different risks.

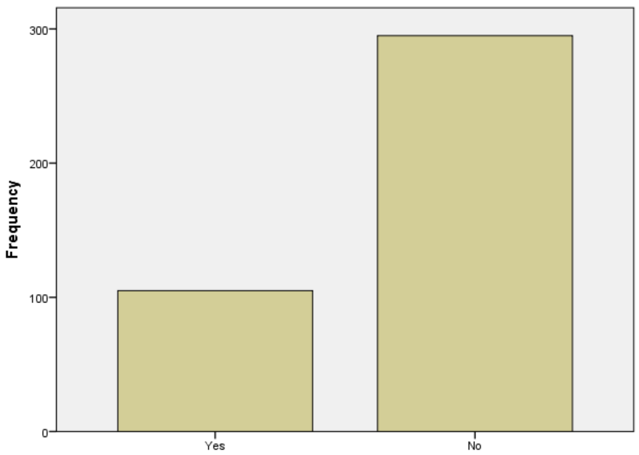


Figure 49. The Ability of Respondents to Access Resources /or Services Off-campus

The results of Question 35 are supported by Gaya (2013) who states that one of the cons of the accessing resources /or services off-campus is slow web connections or older computers that can create accessing course materials frustrating.

Question 36 "Which of the following risks do you think the E-Learning system is prone to?" is focused on the risks that the E-Learning system is prone to. This question also shows how well respondents are familiar with types of risks in E-Learning system.

Table 43. Types of Risks in E-Learning System

	Frequency	Percent	Valid Percent	Cumulative Percent
Hacking	13	3.3	3.3	3.3
Identity Theft	37	9.3	9.3	12.5
Denial of Service	170	42.5	42.5	55.0
Unauthorised modification of course contents	103	25.8	25.8	80.8
Others	77	19.3	19.3	100.00
Total	400	100.0	100.0	

It was important to identify the types of risks that the respondents consider E-Learning is most prone to. The outcomes of this question are outlined in Table 43. The highest percentage of responses is denial of service at 42.5% (n=170), followed by unauthorised modification of course contents at 25.8% (n=103). Only 19.3% (n=73) of responses did not specify the risks and chose the "Others" option, while 9.3% (n=37) of responses pointed out that identity theft is a potential risk and hacking at 3.3% (n=13). Denial of service that was identified by respondents can occur due to multiple reasons but some of them are as follows:

- Connectivity problem;
- Platform incompatibility;

- Server is down (it can be due to maintenance or security intrusion).

The results of Question 36 are also associated with the results of Question 35 that shows that 73.8% (n=295) of respondents are not able to access resources /or services off-campus. Furthermore, Question 36 has significant correlation of .145 at the 0.01 level (2-tailed) with the results of Question 34 (“Are you required to use any other authentication method apart from the password?”). It is obvious that if the E-Learning system does not have strong authentication method, it is vulnerable to different types of risks and threats. Therefore, it is very important for E-Learning system to have the multi-factor authentication method. The outcomes of this question are also supported by our literature review in Chapter 2 (see sub-section 2.11.) where we list the types of vulnerabilities that users encounter while using E-Learning system. We further presented the Classification and Taxonomy of E-Learning Threats (see Chapter 2, sub-section 2.22) and proposed a multi-authentication method with biometrics in order to enhance the Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

5.6. Section 6 of the Questionnaire Survey: Social Awareness

Section 6 of the Questionnaire is focused on the social awareness. The questions within this section also asked for general comments on the survey questionnaires and their willingness to participate in the follow-up studies (e.g. case study / or interview).

Question 37 “It is often said that absolute security is unattainable. To what extent do you agree with this statement?” how the respondents estimate absolute security. Out of 400 responses, 55.5% (n=222) do strongly agree with this statement, 31.8% (n=127) agree, 9.0% (n=36) are neutral and 3.8% (n=15) strongly disagree (see Figure 50). The results of this question can also be associated to the results of Question 29, where out of 400 respondents 98.8% (N=395) of respondents do know that the learning system adopted by their institution can be prone to intrusion by attackers.

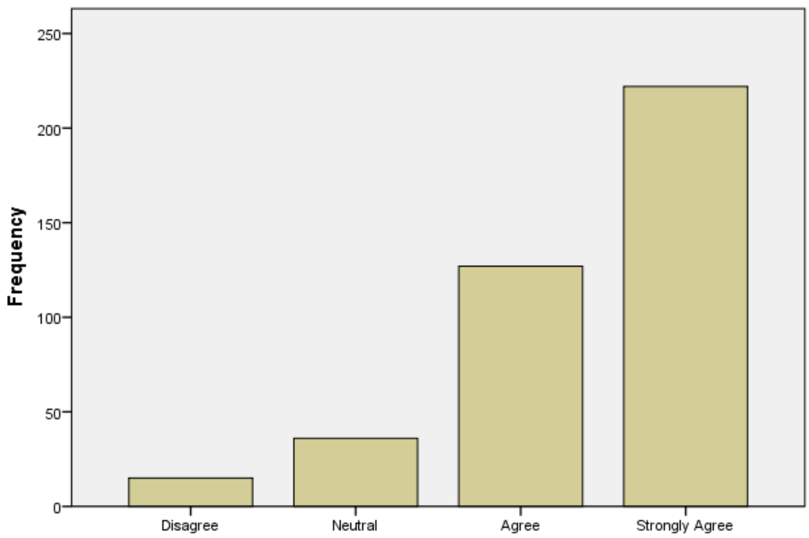


Figure 50. Absolute Security is Unattainable

Moreover, we can also relate the results of this question to the outcomes in Question 36 where respondents show that they are familiar with risks that the E-Learning system is prone to.

Question 38 “What should be done to address the issue of potential loss of confidence by users in the E-Learning system?” tried to find out what can be done to address the issue of potential loss of confidence by users, as the main focus of this study is users’ perception of E-Learning security.

The responses show that an overwhelming 94.8% (n=379) of respondents believe that nothing can be done to address the issue of potential loss of confidence in the E-Learning system. Indeed, out of the total respondents, only 5.3% (n=21) offer various suggestions as to the possible solutions (see Table 44).

Table 44. Addressing the issue of potential loss of users' confidence in the E-Learning system

	Frequency	Percent	Valid Percent	Cumulative percent
None	379	94.8	94.8	94.8
See comments below	21	5.3	5.3	100.0
Total	400	100.0	100.0	

Table 45 shows the 21 responses on how to address the issue of potential loss of confidence by users in the E-Learning system. We specifically grouped these responses into three to show the significant contribution of the respondents’ suggestions.

Table 45. Respondents’ suggestions in relation to the issue of potential loss of users’ confidence

Groups		Suggestions provided by respondents
Group 1	Policy	• Security Policies Implementations • The system should be able to fulfil other security standards • Set security policy • Provide seminars to teach how to use policy • Encouragement of E-Learning innovation • Align sites with best practice • Improvement in software design • To assist in evaluating E-Learning tools
Group 2	Trust	• Build up trust • Establishing standards and regulation that provide a trusted and efficient environment • Employ knowledgeable IT personnel • Deal with reputable service providers
Group 3	Security	• Security Awareness • Log all potential risks • Secure storage of sensitive data • To provide USB authentication tool • Apply multiply authentication models • Understanding the many dimensions of system security • The system must be designed to fend off situations, or deliberate attacks • To add extra level of security and introduce more standardised and flexible risk assessment model • Further development on E-Learning security

As we can see from Table 45, the respondents are concerned about policy, trust and security. The results in Table 45 are the reflection of the respondents' experience and perception that security in E-Learning is still a problem.

Question 39 “Please specify any problems you might have encountered that are not covered in the above sections (e.g. not having a suitable security or risk assessment procedure in your institution/ or company). (If you have not comment(s), please write in “None””. Unfortunately, none of the respondent gave any comments or suggestions to this question.

Question 40 “Would you like to participate in the follow-up studies (e.g. case study/ or interview)?” asked respondents about their willingness to participate in the follow-up studies. Out of 400 respondents 97.3% (n=389) showed their interest in participating in the follow-up studies, and 2.8% (n=11) of respondents did not show any interest.

5.7. Summary of Chapter Five

This study has derived a wealth of data that may be used to understand how important security to E-Learning system. The analysis of six E-Learning case studies and comparing ten existing E-Learning models show that most E-Learning systems that are adopted by higher institutions/ or companies do not have E-Learning security model. Although there is support team at a distance that sometimes can be called upon to rescue minor issues, more often this support team might not be available at the time of needs. Considering the enormous costs involved in creating and maintaining courses, it is unfortunate that security is not yet considered as an important issue by many organisations. Unlike traditional security research, which has largely been driven by military requirements to enforce secrecy, in E-Learning it is not only the information itself that has to be protected but the way it is presented.

The results of 400 completed questionnaires revealed the users' social awareness, their perception of E-Learning security measures, security impacts on the delivery of E-Learning programmes and training, and the risks to which users are exposed to. As E-Learning continues to evolve, the impacts and security issues remain a major concern. The questionnaire survey feedback shows that many other factors are relevant to the successful utilisation of E-Learning and the risk incurred by users. The findings of our study indicate that:

- Security in E-Learning is the main focus for users.
- Some users are not aware of security issues.
- There are weaknesses in the existing E-Learning applications.
- There is lack of multiple authentication methods.

Based on the questionnaire survey feedback, we were able to identify major security risks that E-Learning systems are prone to. As E-Learning increases in popularity and reach, more people run online courses and thus need to understand security issues from a user perspective. We found out from our results that the majority of the respondents appear to understand the severity of the attacks on E-Learning system and importance of E-Learning security in institutions and companies. By addressing the issue of potential loss of users' confidence in the E-Learning system, we received the respondents' suggestions on what major aspects developers and management should focus on in order not to lose users' confidence during online sessions. Our results show that policy, trust and security need to be closely looked at, as the expectations of these aspects among users can affect learning outcomes and learning activities.

Based on the findings and outcomes of this Chapter, we will propose a framework that will address how Access Control and Copyright can enhance security in E-Learning.

Chapter 6: Dynamic E-Learning Access Control and Copyright Framework (DEACCF)

Introduction

The E-Learning system is prone to many security threats as discussed in Chapter 2. After thorough analysis in Chapter 4 which involved six case studies, comparison of ten existing E-Learning models and by conducting a questionnaire survey on Security Issues in E-Learning, we came to conclusion that E-Learning system is very vulnerable, as security in E-Learning is the main focus for users. This chapter focuses on the main aims that were discussed in Chapter 1 which are to investigate how Access control and Copyright can enhance security in E-Learning and to develop a Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

6.1. Proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF)

The DEACCF was proposed for two reasons. The first reason is that the previous frameworks were generally presented as frameworks that were based mostly on single-factor authentication (see Figure 48) or two-factor authentication methods (see Figure 49). The second reason is based on the outcomes of the results of our case studies, existing E-Learning models and results of the questionnaire.

The password-based authentication is not suitable for use on computer networks. Password send across the networks can be intercepted and subsequently used by eavesdroppers to impersonate the user. In addition to the security concern, password-based authentication is inconvenient; user does not want to enter password each time they access the network service (Krishnasamy, 1995). Hackers are constantly searching for ways to compromise passwords using malicious software, phishing scams, and other techniques. If your password is guessed, hacked, or stolen, it can jeopardize your private data as well as University data. Based on the above points, we propose a multifactor authentication method. The MFA adds a layer of security to user’s data by ensuring that the password alone cannot be used to access critical information and services. In our case, it will be difficult if not impossible for an intruder to infringe onto students’ confidential data, exam papers, student results’ alteration avoid unauthorised use of content and add value to Copyright policy. The

MFA is not a luxury but a necessity to give additional security measure to protect users' intellectual property, personal information, and data within the E-Learning system. It adds a stronger access control to the log-in process (see Chapter 2, sub-section 2.18.3).

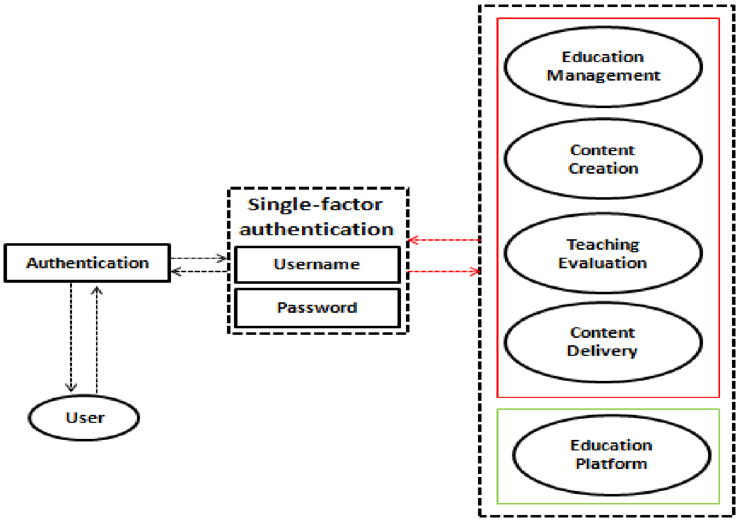


Figure 51. Single-factor Authentication in E-Learning System

Figure 51 shows the metalevel process of single-factor authentication in E-Learning system. The single-factor authentication has been the norm of many system securities for the past decade and still in use as a first gateway prior to other access control mechanisms. The inability of single-factor authentication to stand the pressure of time due to sophisticated hacking tools and the limitations discussed in sub-section 5.6. led to the applicability of Two-factor authentication in E-Learning (see Figure 52).

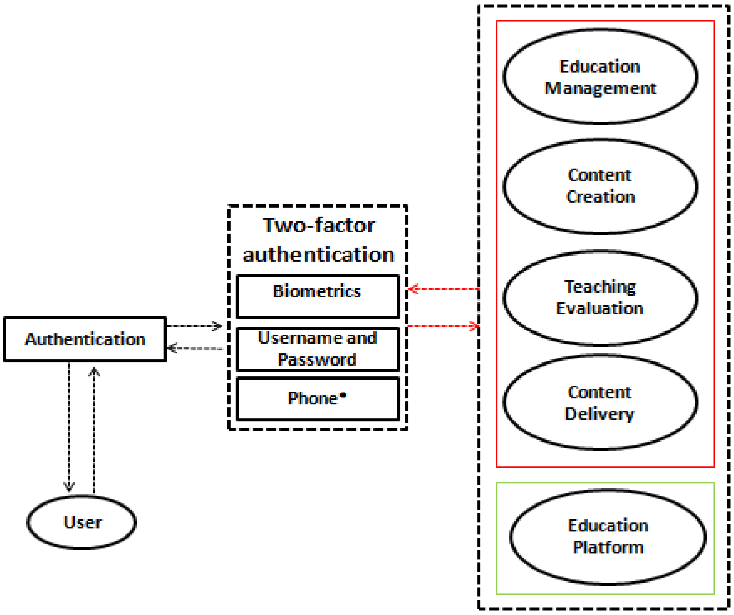


Figure 52. Two-factor Authentication in E-Learning System

The Two-factor authentication came about, as the need for second level Access Control layer became “must have” to mitigate the security breaches from and outside organisation / or institution. The DEACCF is based on the outcomes of the case studies, analysis of the survey questionnaire and weaknesses in the ten commonly used existing E-Learning models. The multi-factor authentication has been integrated to the DEACCF based on the results of the Question 34 in our survey questionnaire, which shows that 83% (n=332) of the respondents were not required to use any other authentication method apart from the password. The results of responses to all the questions in Section 5 of the questionnaire survey show that stronger, reliable and multiple authentication methods are required for secured E-Learning system (see Section 5, sub-section 5.5. for the detailed results). The analysis of six case study observations showed that the organisations used either single- or two-factor authentication with a smartcard. None of the organisations used the multi-factor authentication within their E-Learning system, which proved how weak their Access Control is (see Table 46). We have further analysed ten existing E-Learning models. From the result of the analysis, it is obvious that security was not given consideration at all, and none of the existing models has multi-factor authentication method (see Table 47).

The E-Learning system can be hosted by institution, organisation, service provider, content delivery companies and / or application developer. The proposed DEACCF has three Phases (see Figure 50). The significant contribution of DEACCF is based on the unique selections of the security elements. From the user’s access point the system initiated five combinations of security:

- Biometrics =>Digital Signature => QR Code =>House/Mobile Phone number
- Biometrics => Pattern Recognition => QR Code =>House/Mobile Phone number
- Username / Password => Home/Mobile Phone number => QR Code =>Biometrics
- Digital Signature => QR Code => Home/Mobile Phone number => Biometrics
- Pattern Recognition => QR Code => Home/Mobile Phone number => Biometrics

The above attributes can be prompted in any order. However, the only element that will be in a consistent state is the biometrics enrolment status. The user access point requires multi-dependence attributes as detailed above.

Table 46. Comparative Analysis of the Six Case Study Observations and DEACCF

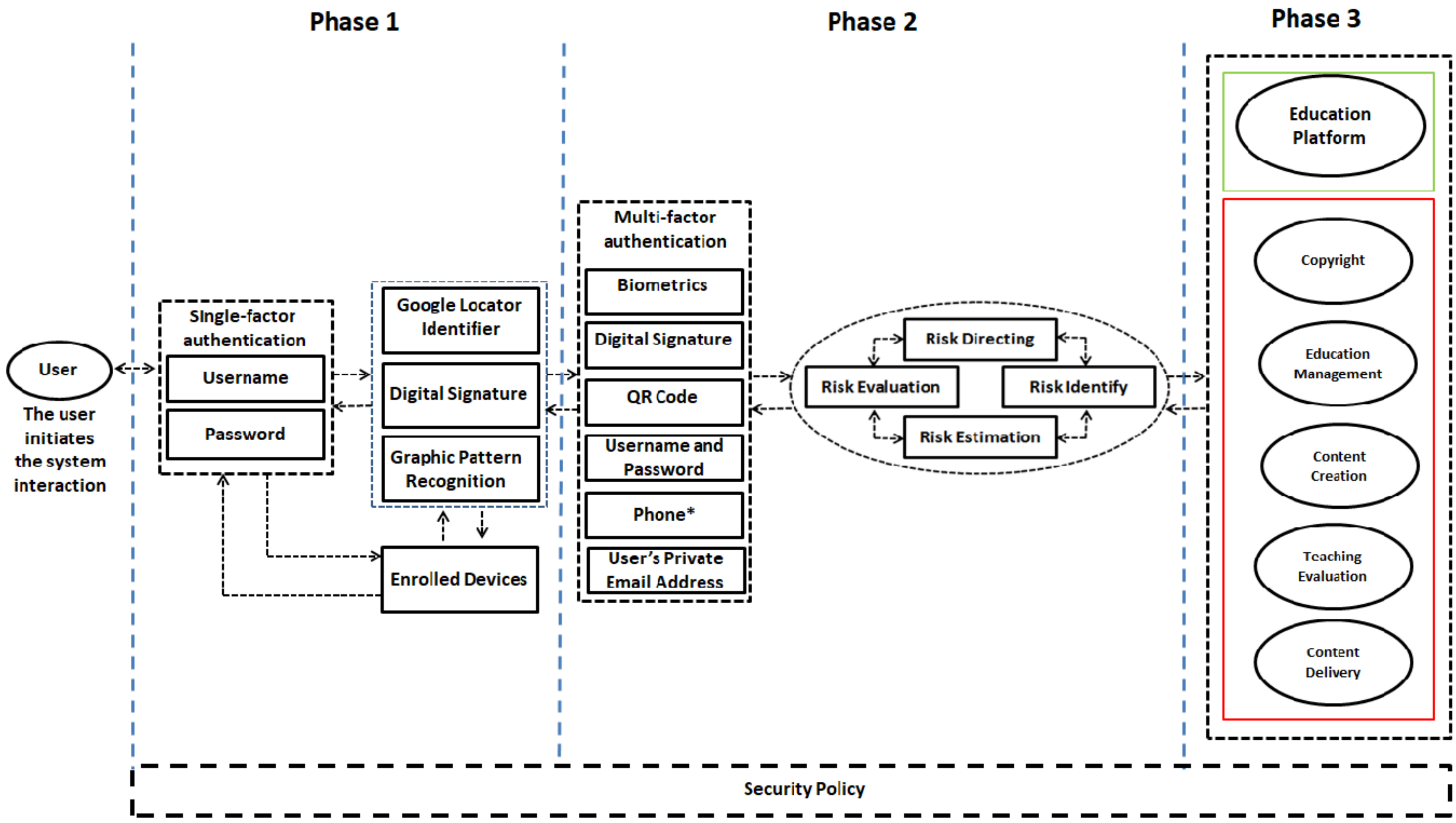
Assessed CSOs Factors	Six Case Study Observations						Proposed Framework
	CSO A	CSO B	CSO C	CSO D	CSO E	CSO F	DEACCF
Type of Access Control:							
- Single-factor authentication	✓		✓	✓	✓	✓	✓
- Two-factor authentication		✓					✓
- Multi-factor authentication							✓
Type of Risk Assessment measures:							
- In-house support							
- Relies on developer							
- Relies on E-Learning software provider	✓	✓	✓	✓	✓	✓	
- Incorporated to the framework							✓
Security Policy							
- Visible to E-Learning Users							✓
- Hidden from E-Learning Users	✓	✓	✓	✓	✓	✓	

*CSO – Case Study Observation

Table 47. Comparative Analysis of the Ten Existing Models and DEACCF

Assessed Models / Factors	Ten Existing Models										Proposed Framework
	1*	2*	3*	4*	5*	6*	7*	8*	9*	10*	DEACCF
Access Control	X	X	X	X	X	X	X	X	X	X	✓
Single-factor authentication	X	X	X	X	X	X	X	X	X	X	✓
Two-factor authentication	X	X	X	X	X	X	X	X	X	X	✓
Multi-factor authentication	X	X	X	X	X	X	X	X	X	X	✓
Security Policy	X	X	X	X	X	X	X	X	X	X	✓
Copyright Policy	X	X	X	X	X	X	X	X	X	X	✓
Biometrics	X	X	X	X	X	X	X	X	X	X	✓
Device Enrolment	X	X	X	X	X	X	X	X	X	X	✓

Key Models	
1* - E-Learning Demand-driven Learning Model	6* - Instructional Design Models for E-Learning
2* - E-Learning Community of Inquiry Model	7* - Anderson and Elloumi's Model of Online Learning
3* - Learning Objects Model	8* - Clark's Model of Instructional Systems Design
4* - Laurillard Conversational Framework	9* - Association for Educational Communications and Technology (AECT) Model of Instructional Technology
5* - Centre for Studies in Advanced Learning Technology (CSALT) Networked Learning Model	10* - International Society for Performance Improvement (ISPI) Model of Human Performance Technology



Phone* (House and/or Mobile Phone Numbers)

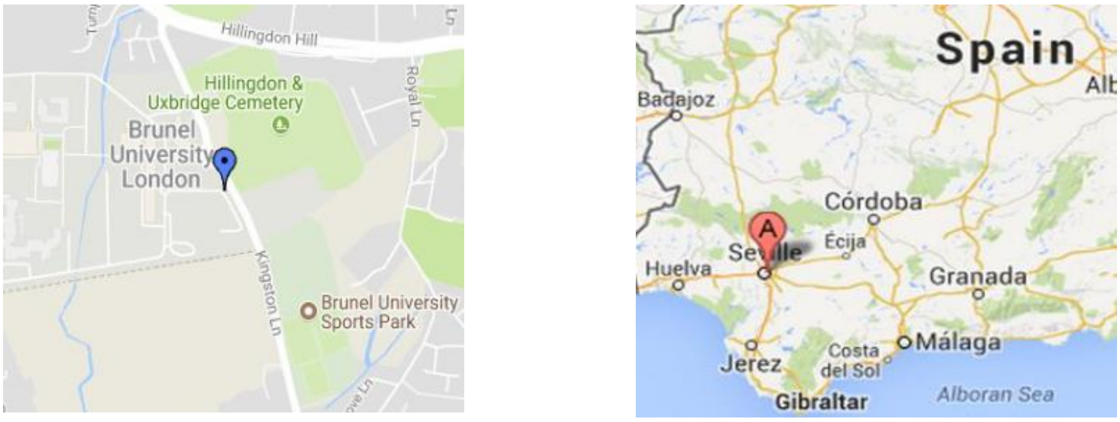
Figure 53. Proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF)

PHASE 1

The single-factor authentication will be incorporated into Phase 1 of the proposed DEACCF. The user signs in using Username and then prompts for Password. The user will be asked to enrol his/her device(s). User can only enrol 4 devices (mobile phone, android, laptop and desktop, or any applicable devices) using device identifier that enables each of the device's serial number / or manufacturer's identification number to be recognised.

- **Google Locator**

The Google locator identifier will deter the security breach by not allowing unauthorised user to login to the E-Learning system. It gives the specific location of the user (see Figure 54). The latter will also enhance Copyright Policy.



(a)

User lives in London, but currently on holidays in Spain

(b)

User's current location is showing in Google map

Figure 54 (a) and (b). Google User's Specific Location

Each time a user is changing location (traveling abroad /or moving to a new location), as long as the address on the system is different, the user will not be able to login. Therefore, the user must update the address on the system 24 hours before any changes can be effective.

- **Digital Signature and Graphic Pattern Recognition**

The digital signature and pattern recognition separately give additional security level and also provide a unique element to the public and private keys that are related. The public key will encrypt the signature and only the corresponding private key can be used to decrypt it. The digital signature uses two keys instead of one key (symmetric encryption).

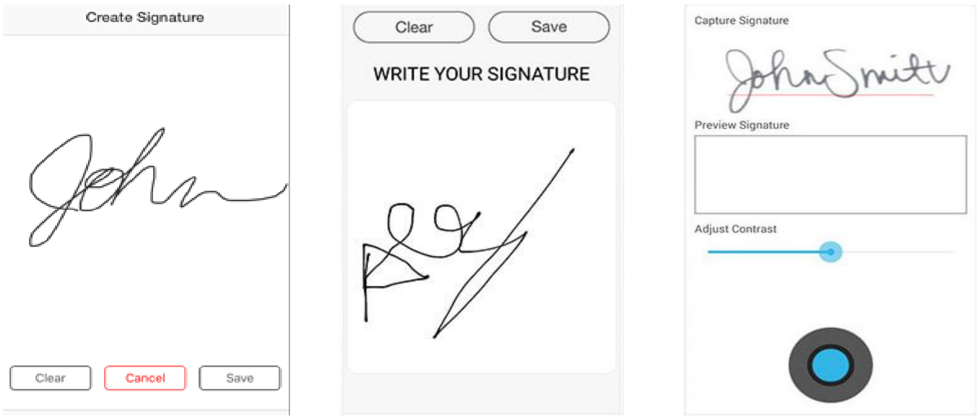


Figure 55. Screen Shot of Digital Signatures

It is virtually impossible to deduce the private key if you know the public key (see Figure 55). The built-in graphic pattern lock tool is useful for adding an extra layer of security to Phase 1 but cannot be used at the same time with the digital signature. The pattern is recorded in a more recognised way to identify any misappropriate space or line (see Figure 56).

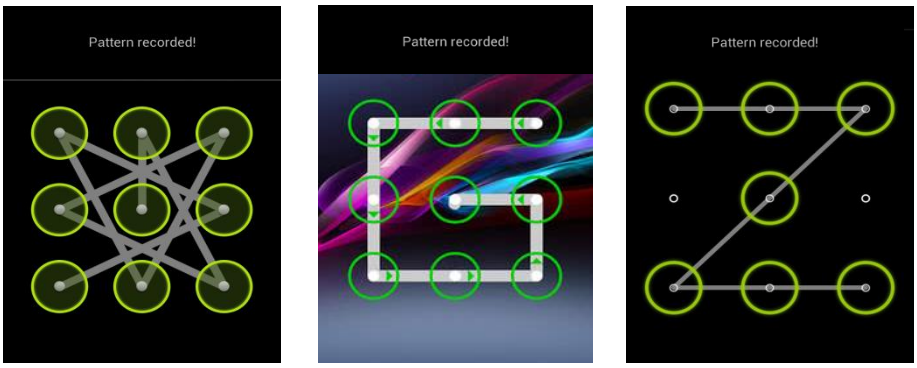


Figure 56. Screen Shot of Graphic Pattern Recognition

User can use the pattern recognition to secure the interaction between their device and the Phase 2.

PHASE 2

The Phase 2 is based on the multi-factor authentication process of matching the attributes that the users provided during the enrolment. The matching attributes initiate combinations of elements and their attributes which are processed in order to verify the user.

- **Biometrics**

The biometrics technology, that has been integrated to the DEACCF, has the ultimate form of electronics security verification of physical attribute of a person. We combined biometrics with other verification attribute, so that the user's specific location and identity can be verified at a given time during and after interacting with the system (see Phases 1 and
2 of DEACCF).

- **Quick Response (QR) Code**

The Quick Response (QR) Code is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan (Denso Wave, 2011). A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used.

Figure 57. QR Code

The QR Code provides the following:
1. High Capacity Encoding of Data
2. Small Printout Size
3. Kanji and Kana Capability
4. Dirt and Damage Resistant
5. Readable from any direction in 360 degrees.
6. Structured Appending Feature

The user will download the QR code reader on his/her mobile phone that will be used to scan the QR code on his/her student's ID card (see Figures 57 and 58).

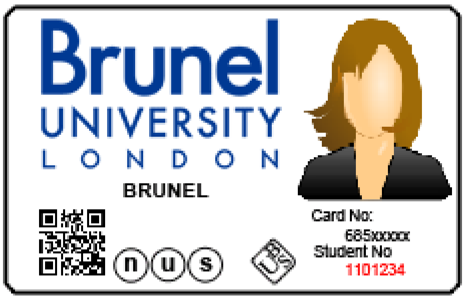


Figure 58. Student’s ID with QR Code

The student’s identity needs to be verified in line with the other sets of Access Control attributes as outlined above.

- **House and/or Mobile Phone**

The DEACCF requires the user to type or input their house (landline) /or mobile phone number that was used during the enrolment. However, if the user enrolled iOS /or Android tablets, they will not be asked to input phone number. The house (landline) /or mobile phone number are equally important when authenticating the user’s legitimate access control.

- **User’s Private Email Address**

The user’s private email address is used for further verification. The user will be instructed to login to the private email address provided in order to click on the verification code. The latter will accept the verification code. All other things being equal, the Access Control set of attributes should and must be verified without any error.

- **Risk Assessment Process**

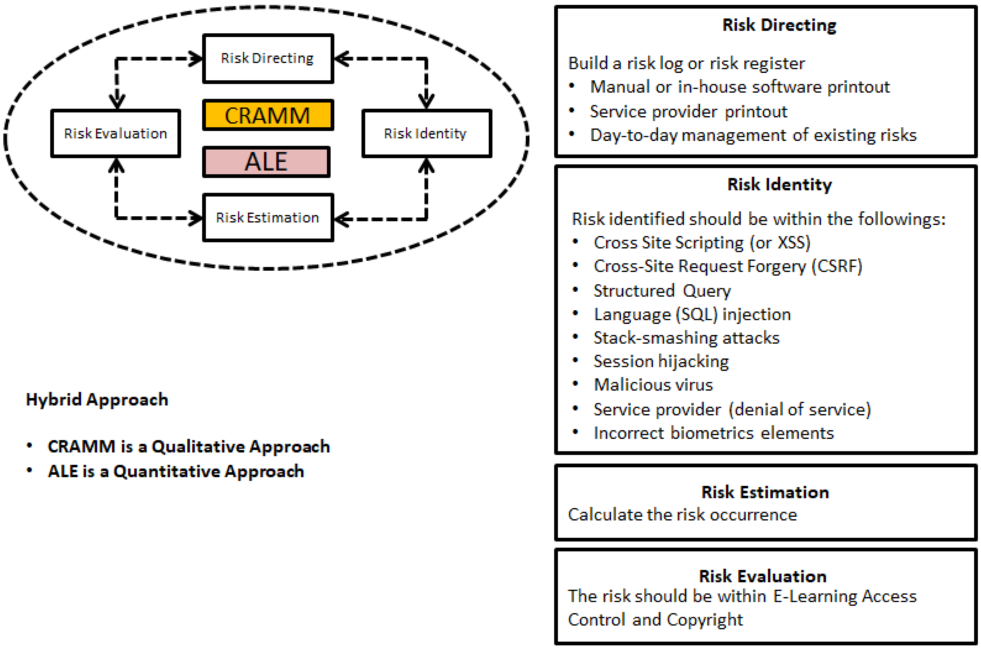
The risks of any security breaches while trying to login are mitigated by the risk assessment process as shown in the DEACCF (see Figure 53). The Hybrid Approach Risk Assessment Model is based on Quantitative and Qualitative Approaches (see Figure 59). The questionnaire survey findings in Chapter 5 Section 5.3 show that there is an urgent need for an appropriate risk assessment approach in place that can be used to tabulate associated numerical security risk to financial /or cost implication to the institution /or organisation.

PHASE 3

Phase 3 is the final stage of the DEACCF, which consists of the "Education Platform" that processes the data generated from E-Learning materials (see Figure 53 - Proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF)). The Copyright elements relating to the proposed framework have been discussed in sections 2.12 and 2.20, and it was suggested that copyright should be based on trust from all parties involved in the development and the dissemination of the E-Learning materials. Based on the questionnaire's results in Chapter 5 sub-section 5.4, it is obvious that Copyright should be given serious attention as the Internet boundaries are unquestionable and the security policies need constant review.

6.2. E-Learning Security Threats Risk Assessment Model

An E-Learning Security Threats Risk Assessment Model based on hybrid approach has been incorporated to DEACCF to mitigate the Access Control security breaches during and after the user's login (see Figure 59).



Hybrid Approach

- **CRAMM is a Qualitative Approach**
- **ALE is a Quantitative Approach**

Risk Directing

Build a risk log or risk register

- Manual or in-house software printout
- Service provider printout
- Day-to-day management of existing risks

Risk Identity

Risk identified should be within the followings:

- Cross Site Scripting (or XSS)
- Cross-Site Request Forgery (CSRF)
- Structured Query
- Language (SQL) injection
- Stack-smashing attacks
- Session hijacking
- Malicious virus
- Service provider (denial of service)
- Incorrect biometrics elements

Risk Estimation

Calculate the risk occurrence

Risk Evaluation

The risk should be within E-Learning Access Control and Copyright

Figure 59. E-Learning Security Threats Risk Assessment Model

6.2.1. Qualitative Approach: CRAMM

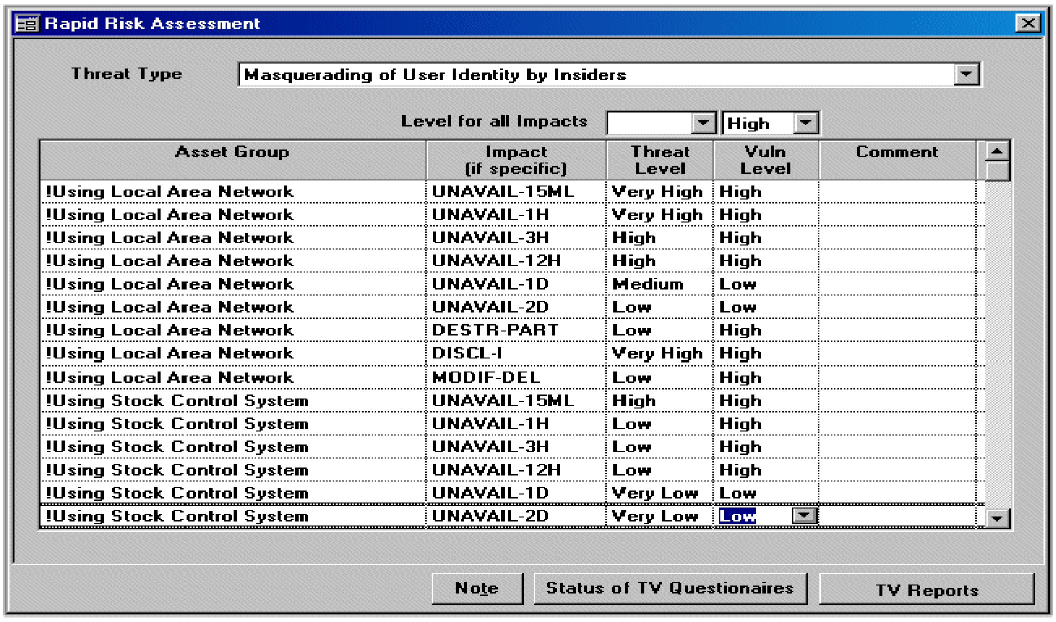
The qualitative approach uses CRAMM (Central Computing and Telecommunications Agency (CCTA) Risk Analysis and Management Method), which is ISO/IEC 27001 compliant (see Chapter 2, sub-section 2.10). The CRAMM method consists of three stages, each supported by questionnaires and guidelines. Each stage aims to answer one or two significant questions as follows:

Stage One - Is the value of assets (consisting of hardware, software and data) high enough to warrant security procedures more stringent than the use of a general ‘code of good practice’?

Stage Two - What and where is the security need?

Stage Three - How can the need be met?

CRAMM contains a range of documents (such as a recommended security policy and management report) that can be used to formalize security policy. At the core of CRAMM is the rapid risk assessment (see Figure 60 below).



Rapid Risk Assessment

Threat Type: Masquerading of User Identity by Insiders

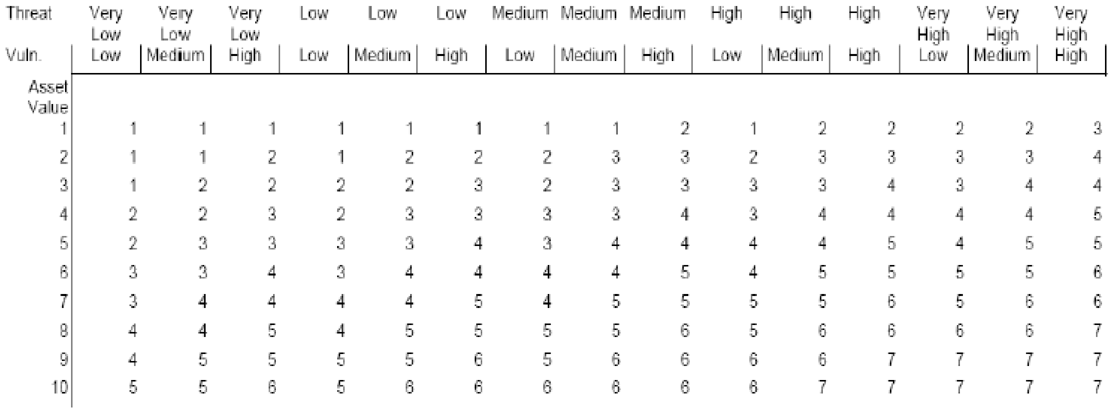
Level for all Impacts: High

Asset Group	Impact (if specific)	Threat Level	Vuln Level	Comment
!Using Local Area Network	UNAVAIL-15ML	Very High	High	
!Using Local Area Network	UNAVAIL-1H	Very High	High	
!Using Local Area Network	UNAVAIL-3H	High	High	
!Using Local Area Network	UNAVAIL-12H	High	High	
!Using Local Area Network	UNAVAIL-1D	Medium	Low	
!Using Local Area Network	UNAVAIL-2D	Low	Low	
!Using Local Area Network	DESTR-PART	Low	High	
!Using Local Area Network	DISCL-I	Very High	High	
!Using Local Area Network	MODIF-DEL	Low	High	
!Using Stock Control System	UNAVAIL-15ML	High	High	
!Using Stock Control System	UNAVAIL-1H	Low	High	
!Using Stock Control System	UNAVAIL-3H	Low	High	
!Using Stock Control System	UNAVAIL-12H	Low	High	
!Using Stock Control System	UNAVAIL-1D	Very Low	Low	
!Using Stock Control System	UNAVAIL-2D	Very Low	Low	

Figure 60. Screenshot of One of CRAMM’s Analysis

The accumulated threats in Table 48 can be used to assess the impact of changes and as information resource for making further decisions with regards to the threat level and how it can be improved.

Table 48. Screenshot of Analysis of Vulnerability Threats



Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

The analysis in Table 48 shows the severity of impacts which is compared with an appropriate guideline, providing value within the scale of 1 to 7 which is ranged from "Very Low" to "Very High". These numbers are used in Annualised Loss Expectancy (ALE) to quantify each number to a financial value (see Table 49).

6.2.2. Quantitative Approach: ALE

ALE (Annualised Loss Expectancy)

The annualised loss expectancy (ALE) value approach is determined by the following elements:

- Determine the financial value of the assets or resources at risk
- Determine the exposure factor – that is, the percentage of the asset value at risk
- Compute the single loss expectancy:

Single loss expectancy = Financial value × Exposure factor

- Determine the annualised rate of occurrence – that is, the reciprocal of the average number of years between incidents of the risk
- Determine the annualised loss expectancy (ALE):

ALE = SLE × ARO

ALE = Single loss expectancy × Annualised rate of occurrence

ARO = Annualised Rate of Occurrence. (How often it happens per year)
SLE = Single Loss Expectancy. (How much a single-loss costs)
SLE may be calculated using EF (Exposure Factor)

6.2.3. Mapping CRAMM to ALE

The different levels in CRAMM and ALE can be mapped to concrete values. The example for mapping levels of risk to ALE is shown in Table 49.

Table 49. Vulnerability Threats Values

CRAMM Measure of Risk	Annual Loss of Expectancy (ALE)
1	< £1,000
2	< £10,000
3	< £100,000
4	< £1,000,000
5	< £10,000,000
6	< £100,000,000
7	< £1,000,000,000

The outcomes of our questionnaire survey (see Chapter 5 sub-section 5.3) show that there is a need for E-Learning system to have the vulnerability threat values assigned to specific threat type. Based on the latter, we have implemented the mapping of CRAMM to ALE in our DEACCF (see Figures 56 and 59).

6.3. DEACCF Validation

The DEACCF was validated by sending the questionnaire titled “DEACCF Validation” to E-Learning developers in UK (see Appendix B). The total number of questionnaire feedbacks is 21. The developers’ contact email addresses were sourced out from the Internet website called Learning Light (Srivastava, 2018). The participants were purposefully selected based on their experience in developing E-Learning systems. It was anticipated that these participants would provide the most valuable feedback.

The initial contact with the developers was based on telephone calls to their respectful companies. It took longer than expected to identify the appropriate person that will be interested in helping to validate our proposed framework. After accepting to participate in the survey questionnaire titled "DEACCF Validation Questionnaire" (see Appendix B), the participants were asked the following questions (the results are presented in Table 50):

- What is your Age?
- What is your Gender?
- What is your Job Role?
- Number of years as an E-Learning developer.

Table 50. Participants' Data Findings Based on Telephone Conversion

Age	How many participants within the Age range?	Gender	Number of years as an E-Learning developer?	Participant's Job role
33	1	Male	7	E-Learning Developer
35	3	Male	8	E-Learning Developer and Tester
37	2	Female	10	E-Learning Developer and Instructional Designer
39	4	Male	8	E-Learning Developer and Script Validation Specialist
40	3	Male	10	E-Learning Developer
42	1	Female	6	E-Learning Developer and Script Validation Specialist
44	3	Male	9	E-Learning Developer and Tester
45	4	Male	10	E-Learning Developer and Tester

All participants that were selected to validate the framework are between the age of 30 to 45 (see Table 50). The results of the Table also show that very few Females are currently involved in E-Learning development. The total response shows that only 3 Females out of 21 participants with the rest 18 participants accounted for as Male. The participants' number of years as E-Learning developers is between 6 to 10 years: 9 out of 21 participants have 10 years of experience, 3 with 9 years of experience, 7 with 8 years of experience, 1 with 7 years of experience and 1 participant with 6 years of experience. All participants have the same job role as an E-Learning developer; however, some of them have additional responsibilities as Tester, Script Validation Specialist and Instructional Designer.

The first introduction to DEACCF and the importance of having it validated was part of our initial discussion during the telephone conversation. The latter was consequently backed by an email with the detailed description of the proposed framework (see Appendix C).

The results of the DEACCF Validation Questionnaire show that out of 21 respondents the 85.7% (n=18) respondents will propose using DEACCF in their organisations with some changes. The 14.2% (n=3) respondents will not consider using DEACCF to develop client's E-Learning system because of the following reasons:

a. Biometrics issues: not all users are willing to share their biometrics elements due to religious reasons.
b. Budget restrictions: in most organisations / or companies' budget is allocated on how much is needed to be spent on enhancing the E-Learning system(s). If the cost of implementing DEACCF exceeds the allocated annual budget, it will discourage the adaptation of the framework.
c. Too many levels of security /or security gateway will lead to low speed in executing the E-Learning system.

6.4. Outcomes of Hypotheses

Based on the literature review (see Chapter 2), analysis of the six case studies observations and ten existing models (see Chapter 4), results of our questionnaire survey (see Chapter 5) we were able to prove our hypotheses as follows:

Hypothesis 1:

- Null hypothesis $\left(H_0^1\right)$: Access Control is unattainable in the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF).
- Alternative $\left(H_A^1\right)$: Access Control is attainable in the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

Null hypothesis $\left(H_0^1\right)$ is rejected in favour of Alternative hypothesis $\left(H_A^1\right)$.

Based on the results of our investigation, Access Control is attainable in the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF) (see Chapter 6, sub-section 6.1).

Hypothesis 2:

- Null hypothesis $\left(H_0^2\right)$: The proposed Risk Assessment Model is unattainable in securing the Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

- Alternative $\left(\mathrm{H}_{\mathrm{A}}^{2}\right)$: The proposed Risk Assessment Model is attainable in securing the Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

Alternative $\left(\mathrm{H}_{\mathrm{A}}^{2}\right)$ rejects Null hypothesis $\left(\mathrm{H}_{0}^{2}\right)$.

The analysis of our findings disproved Null hypothesis $\left(\mathrm{H}_{0}^{2}\right)$ and accepted Alternative $\left(\mathrm{H}_{\mathrm{A}}^{2}\right)$ By proposing the E-Learning Security Threats Risk Assessment Model which is based on hybrid approach we have proved that risk assessment is attainable in securing the Dynamic E-Learning Access Control and Copyright Framework (DEACCF) (see Chapter 6, sub-section 6.2).

6.5. Summary of Chapter Six

This study has derived a wealth of data that may be used to understand how important security to E-Learning system. The analysis of six E-Learning case studies and comparing ten existing E-Learning models show that most E-Learning systems that are adopted by higher institutions/ or companies do not have E-Learning security model. Although there is support team at a distance that sometimes can be called upon to rescue minor issues, more often this support team might not be available at the time of needs. Considering the enormous costs involved in creating and maintaining courses, it is unfortunate that security is not yet considered as an important issue by many organisations. Unlike traditional security research, which has largely been driven by military requirements to enforce secrecy, in E-Learning it is not only the information itself that has to be protected but the way it is presented.

The results of 400 completed questionnaires revealed the users' social awareness, their perception of E-Learning security measures, security impacts on the delivery of E-Learning programmes and training, and the risks to which users are exposed to. As E-Learning continues to evolve, the impacts and security issues remain a major concern. The questionnaire survey feedback shows that many other factors are relevant to the successful utilisation of E-Learning and the risk incurred by users. The findings of our study indicate that:

- Security in E-Learning is the main focus for users.
- Some users are not aware of security issues.
- There are weaknesses in the existing E-Learning applications.

- There is lack of multiple authentication methods.

Based on the questionnaire survey feedback, we were able to identify major security risks that E-Learning systems are prone to. As E-Learning increases in popularity and reach, more people run online courses and thus need to understand security issues from a user perspective. We found out from our results that the majority of the respondents appear to understand the severity of the attacks on E-Learning system and importance of E-Learning security in institutions and companies. By addressing the issue of potential loss of users' confidence in the E-Learning system, we received the respondents' suggestions on what major aspects developers and management should focus on in order not to lose users' confidence during online sessions. Our results show that policy, trust and security need to be closely looked at, as the expectations of these aspects among users can affect learning outcomes and learning activities.

Based on the findings and outcomes of this Chapter, we have proposed a framework that addressed how Access Control and Copyright can enhance security in E-Learning. The security of E-Learning system should be designed with multiple architectural layers and trust boundaries that will determine the interaction rates of any software and hardware components. The questionnaire survey results show that there is a lack of awareness about E-Learning security issues in UK educational institutions /or organisations, which also includes the use of third-party materials.

Chapter 7: Conclusion

Introduction

This chapter provides the conclusion to this research work by presenting the main achievements and contributions and highlighting the limitations experienced and discussing future work. Sub-section 7.1 addresses how the objectives of our research work were achieved and the justification of the research questions. Sub-section 7.2 highlights the contribution of this research to the body of knowledge, while Sub-section 7.3 describes how the DEACCF can be integrated to existing E-Learning systems. Sub-section 7.4 outlines the cost implications and learner friendliness of the DEACCF. Sub-section 7.5 provides a review of the main limitations. Finally, sub-section 7.4 confers the potential for further development.

7.1. Research Conclusion

After developing a background context for the research, the research questions were defined, from which the research aims and objectives were drawn in Chapter 1. This research has been undertaken to investigate how Access Control and Copyright can enhance security in E-Learning. This research achieved the following objectives:

1. To identify what precisely constitute security threats in E-Learning.

2. To produce classification and taxonomy of E-Learning Security threats that will help in identifying the specific security risks.

3. To explore Access Control and Copyright measures in E-Learning.

4. To review the existing E-Learning models in order to understand the limitations of current Access Control and Copyright issues.

5. To develop a Dynamic E-Learning Access Control and Copyright Framework (DEACCF) based on the results and limitations obtained from the existing models, case studies and questionnaire.

6. To propose a multi-authentication method with biometrics in order to enhance the Dynamic E-Learning Access Control and Copyright Framework (DEACCF).

The first objective was met through a comprehensive literature review (see Chapter 2, sub-section 2.11), which addressed “What precisely constitutes security in E-Learning?” by exploiting the conceptual understanding of E-Learning, benefits and challenges, types of E-Learning (distinctive features and examples of technologies in Synchronous and Asynchronous E-Learning), information security in relations to E-Learning, legislations, Copyright as security issues in E-Learning and application security problems.

The second objective was achieved by producing the classification and taxonomy of E-Learning Security threats. It was developed to identify the specific security risks that a user can encounter (see Chapter 2, sub-section 2.22).

The third objective was achieved through the descriptive study, which reviewed all available models of Access Control and Copyright in general, in order to understand how the latter can enhance security in E-Learning (see Chapter 2, sub-sections 2.13 and 2.14).

The fourth objective was achieved through the descriptive study, which analysed six E-Learning case studies observations and compared ten existing E-Learning models (see Chapter 4). The exploratory study was also involved, which investigated the public opinion in relation to the security, attitude and awareness of E-Learning with a questionnaire survey of 400 respondents. It was distributed to academic institutions and commercial sectors in the United Kingdom. The study also helped to identify the security issues in E-Learning (see Chapter 5).

The fifth objective was achieved through the development of Dynamic E-Learning Access Control and Copyright Framework (DEACCF) based on the results and limitations obtained from the six case studies observations, ten existing models and questionnaire survey (see Chapter 6, sub-section 6.1).

The sixth objective was achieved by proposing a multi-factor authentication method (see Chapter 6, sub-section 6.1, Phase 2) and incorporate E-Learning Security Threats Risk Assessment Model based on hybrid approach to enhance DEACCF (see Chapter 6, sub-section 6.2).

The justification of the research questions stated at the outset of the thesis are discussed below:

Our first question “What precisely constitutes security in E-Learning?” has been answered thorough research in available literatures (see Chapter 2) and questionnaire survey (see Chapter 5). We also looked into the security requirements and vulnerabilities that are currently encountered within E-Learning systems.

The second question “Is classification and taxonomy of E-Learning security possible?” has been answered by analysing the security threats in E-Learning and proposing the Classification and Taxonomy of E-Learning Security Threats (see Chapter 2, sub-sections 2.12, 2.13 and 2.20).

We were able to answer the question “What constitutes the failure of E-Learning technologies?” by reviewing the available literature and results of the questionnaire survey (see Chapter 2, sub-section 2.7.5 and Chapter 5).

The analysis of literature review, six case studies observations, ten existing E-Learning models and the results of the questionnaire survey have shown that learning content is not secure when using E-Learning. Based on the latter, we proposed the Dynamic E-Learning Access Control and Copyright Framework (DEACCF) to secure content within E-Learning system (see Chapter 2, Chapter 4, Chapter 5 and Chapter 6).

Finally, after proposing the DEACCF, we have incorporated an E-Learning Security Threats Risk Assessment Model based on hybrid approach to our framework. The latter has answered question five “Is there any risk assessment model that can be used to assess the possible risk incurred by E-Learners?” (see Chapter 6, sub-section 6.2).

7.2. Contribution to Knowledge

The key contributions of this thesis are as follows:

7.2.1. Identifying the research gap

Chapter Two reviewed studies related to the security issues in E-Learning and identified the limitations in this field. The current literature lacks a focus on security and privacy enhancement of Copyright in E-Learning. The current thesis therefore explores studies in Copyright in relation to E-Learning and its links to security and privacy enhancement within E-Learning.

7.2.2. Current state of security issues in E-Learning

The detailed evaluation was conducted with a questionnaire survey of 400 respondents from academic institutions and commercial sectors in the United Kingdom. The questions were selected carefully; the participants were ensured to have a long and direct experience with E-Learning system. The rationale for this purposive selection was to ensure that the questionnaire covers users, instructors and developers. This part of the research was to investigate the security threats to which E-Learning is exposed and how to assess the threats (see Chapter 5).

7.2.3. Analysis of the usability of single and multifactor authentications

The exploratory study in Chapter 6 showed different authentication methods, including single and multi- factor authentications. An analysis to comparing the usability and security between single and multifactor authentication was conducted. The results provided a clear picture of the high security of multifactor authentication on the basis of the perceptions of users who have a long experience in using both methods (see Chapter 6).

7.2.4. Analysis of different authentication methods

A comprehensive and extensive analysis of nine popular authentication methods was conducted. The study pointed out that a biometric method should be included to achieve new and logical evaluation results (see Chapter 2).

7.2.5. Proposed Dynamic Framework

The development of the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF) has led to more secure Access Control based on our multi-factor authentication which involves Biometrics, Digital Signature, QR Code, Username and Password, Phone and User's Private Email Address. The proposed framework will enhance user’s security level and protect personal information and data within E-Learning system.

Within the proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF) we have in-cooperated E-Learning Security Threats Risk Assessment Model which is based on hybrid approach (see Chapter 6, sub-sections 6.1 and 6.2).

7.3. Integrating DEACCF to Existing E-Learning Systems

The DEACCF is extremely flexible to integrate the required Phases to any E-Learning system. For example, if the current system is based on Single-Factor Authentication, the first part of Phase 1 (username and password) will not be required. Therefore, we only need to integrate the Google Locator Identifier, Digital Signature and Graphic Pattern Recognition that will be linked to the enrolment devices. The enrolment devices will be triggered by the Single-Factor Authentication to initiate the process of logging in (see Phase 1 of the DEACCF). The latter process is also applied to Two-Factor Authentication. Multi-Factor Authentication is not platform dependant. As long as Phase 1 is already in existence within the E-Learning system, the Phase 2 is an interface that enables the Phase 1 to recognise the process in place (see Phase 2 of the DEACCF).

7.4. Cost Implications and Learner Friendliness

Many institutions and companies give a huge consideration to cost and do not want to spend more than allocated budget to deploy a new function into their E-Learning system. It is important to balance usability, cost and security in order to enhance the user experience without alienating their user base.

The proposed DEACCF is very cost-effective, as it is a low maintenance integration and will not require a yearly licence. The biometrics aspect of the system is extremely competitive and the cheapest biometrics device costs less than £25.00 to effectively function with other parts of the framework. Implementing the whole system from start to finish (from Phase 1 to Phase 3) will cost less than £2000.00 depending on the number of users. However, the cost effectiveness can also be related to the ease of use.

The DEACCF is a very robust framework that does not require an expert’s skill, as most of the applications that are integrated within the system can be purchased separately with the capability of working across multi-platform. Furthermore, our framework does not require any code alteration or programme language specific.

7.5. Limitations

Like in any other research, there are several limitations that need to be mentioned. The limitations that are outlined below can be very helpful for future research:

1. Due to the time factor, we were unable to implement our proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF). However, we opted for industrial validation of the framework.

2. The DEACCF is very robust to be implemented but culture, relegation and government policy can hinder the adaption of our framework in other countries.

3. The questionnaire survey can be further extended to all universities, colleges and companies in the United Kingdom, as this will give broader and comprehensive results.

4. E-Learning is now becoming part and parcel of institutional and industrial programmes / training that many countries around the world are embracing. Unfortunately, due to the time factor of our research we did not have the opportunity to extend our research (specifically questionnaire survey) to other countries. Increasing the number of population of participants in the questionnaire survey in other countries' institutions / organisations that are currently using E-Learning will enhance the generalisability and give better overall results.

5. Implementing Copyright into E-Learning system is a challenging area, as universities, colleges or companies have different Copyright Policy. It is difficult to unify the Copyright Policies into a standard that will be withheld to across the board in the digital society.

6. The boundaries between trust and Copyright demand clarity from all parties involved in the development and the dissemination of the E-Learning materials.

7. The validity of our questionnaire survey results can be said to be inconclusive due to the geographical locations of our respondents. The results would have been different if the questionnaire survey was conducted among all the Universities and organisations in the UK / or UK and other countries.

8. Even though we have tested our questionnaire survey, it is inevitable that the reliability of this research will always be a concern, as we did not conduct the same survey more than once. The reliability of the results would have been sustainable if we conducted the same questionnaire survey several times. For this reason, we cannot conclude that the results will stay the same overtime to achieve the expected reliability.

7.6. Future Work

It is noted that many other factors are relevant to the successful utilisation of E-Learning system from user's perspective and the risk assessment of encountered threats. As the delivery of educational modules and training using E-Learning continues to evolve, the Access Control and Copyright in E-Learning from user's perspective in the United Kingdom remain a major concern. This does not apply to the E-Learning developers only (which have already been investigated and researched within our study), but also to other service providers such E-Learning contents providers. Therefore, there is a future need to expand the limitation of our research area to include the E-Learning contents providers that are currently delivering the service within other service providers' domains. We believe that further work in this area will enhance the future understanding of the Access Control and Copyright in E-Learning and types of threats that can be associated to the service.

Based on the results of the questionnaire survey, there seems to be security policies gap between all parties involved in the development and the dissemination of the E-Learning materials. Future research can bridge the gap by proposing different approaches that can help to translate the security policies into requirements for the E-Learning developers.

Glossary

AECT	Association for Educational Communications and Technology
ALE	Annualised Loss Expectancy
ARIADNE	Alliance of Remote Instructional Authoring and Distribution Networks for Europe
ATM	Automated teller machine
BBA	Biometrics-Based Authentication
DEACCF	Dynamic E-Learning Access Control and Copyright Framework
CA	Certificate Authority
CBT	Computer-based Training
CCTA	Central Computing and Telecommunications Agency
CETADL	Centre for Educational Technology and Distance Learning
CMI	Computer Managed Instruction
CRAMM	Central Computing and Telecommunications Agency Risk Analysis and Management Method
CSALT	Centre for Studies in Advanced Learning Technology
CSO	Case Study Observation
CSRF	Cross-Site Request Forgery
CSS	Cross Site Scripting
DAC	Discretionary Access Control
DCML	Data Center Markup Language
DMZ	Demilitarized Zone
DSI	Dynamic Systems Initiative
DVD	Digital Optical Disc
eSignature	Electronic Signature
ESF	European Social Fund
FBA	Formula-Based Authentication

GPS	Global Positioning System
HPT	Human Performance Technology
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICT	Information and communications technology
ID	Identity Document
IEEE	Institute of Electrical and Electronics Engineers
IMS	Instructional Management Systems
IP	Internet Protocol
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISPI	International Society for Performance Improvement
ITU	International Telecommunication Union
KBA	Knowledge-Based Authentication
LAN	Local Area Network
LBA	Location-Based Authentication
LIP	IMS Learner Information Package
LMS	Learning Management Systems
LSS	Location Signature Sensor
LOM	Learning Object Metadata
LTSC	Learning Technology Standards Committee
MAC	Mandatory Access Control
MFA	Multi-Factor Authentication
M-Learning	Mobile Learning
Moodle	Modular Object-Oriented Dynamic Learning Environment
NIST	National Institute of Standards and Technology

OOHDM	Object Oriented Hypermedia Design Method
OS	Operating System
OTP	One-Time Password
PAPI	Public and Private Information
PBA	Process-Based Authentication
PC	Personal Computer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRS	Personal Response System
QR	Code Quick Response Code
RBA	Relationship-Based Authentication
RBAC	Role-Based Access Control
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
SysML	Systems Modeling Language
TAN	Transaction Authentication Number
TBA	Token-Based Authentication
TCP	Transmission Control Protocol
TCPE	Tachyon Customer Premises Equipment
TEL	Technology Enhanced E-Learning
TMAC	Team-Based Access Control
TPM	Trusted Platform Module
TSP	Trust Service Provider
UML	Unified Modeling Language
URL	Uniform Resource Locator

USB	Universal Serial Bus
UWE	UML-based Web Engineering
VLE	Virtual Learning Environment
WAN	Wide Area Networks
WebML	Web Modeling Language
WLAN	Wireless Local Area Network
WSDL	Web Service Description Language
XML	Extensible Markup Language
XSS	Cross Site Scripting

Appendix A: Security Issues in E-Learning Questionnaire Survey

Security Issues in e-Learning Survey

In the understanding that you are a busy professional, 10 minutes of your time is being sought to contribute to the knowledge gap within ’Security Issues in e-Learning’. On completion of the study, a copy of the summary of findings will be sent to you (it is anticipated that this will contain views from a wide spectrum of companies who have developed e-Learning applications).

Neither confidential information nor any company's details are being sought in the questionnaire; instead the aim is to collate security issues in e-Learning and explore the risk assessment models that are currently in use to assess e-Learning breaches.

Please note that this is an academic research survey, and NOT a marketing or product survey.

---

1. General information

Q1. Are you associated with a higher educational institution?
(If not, go to Q. 8)

□ Yes
□ No

Q2. Which of the following categories best describes your role in your institution:
(If you are a student, go to Q. 6)

□ a. Lecturer
□ b. Administrator
□ c. Manager
□ d. Technician
□ e. Other (please describe)

□

Q3. Do you use e-Learning as part of your teaching or professional practice?
(If no, go to Q8. and continue)

□ Yes
□ No

Q4. Do you develop e-Learning applications?

□ Yes
□ No

If yes, what type?

Q5. Do you train people on how to use the e-Learning applications?

□ Yes
□ No

Q6. Are you a student in higher education? Please indicate which of the following applies to you. (If you are not a student, please go to Q. 8)

□ a. Full-time student
□ b. Part-time student
□ c. Distance learner
□ d. Leisure learner
□ e. Other (please specify)

Q7. If you are a student, do you use e-Learning as part of your mode of learning?

□ Yes
□ No

2. The impacts of e-Learning on the delivery of your programme(s)

Q8. What type of learning approach has been adopted by your institution /or company?
(Select all that apply)

□ a. Traditional training
□ b. e-Learning
□ c. Training courses
□ d. Blended Learning (if Blended Learning, please select all that apply)

○ Classroom Learning
○ Online Learning
○ Mobile Learning

□ e. Other (please specify)

9. What types of technology do you use within your e-Learning environment?
(Select all that apply)

□ a. E-mail
□ b. Voice Mail
□ c. Scanner
□ d. Facsimile Application
□ e. Webinars
□ f. Teleconferencing
□ g. Data Conferencing
□ h. Video Conferencing
□ i. Mobile phone
□ j. Telephone
□ k. Other (please specify)

Q10. From your experience, what are the impacts of e-Learning on your programme(s) / training? (Select all that apply)

□ a. Increasing speed with which teaching materials can be obtained
□ b. Increasing speed with which learning materials can be shared
□ c. Reduced operating costs
□ d. 24 hours a day, 7 days a week availability
□ f. Access to search and retrieval systems
□ g. Global accessibility from all over the world
□ h. Promote products to suit each individual learner
□ i. Other (Please write in)

Q11. What do you consider the top 3 reasons for not using the available e-Learning tools? (Please tick three)

□ a. Lack of tutor support / readily available contact
□ b. Absence of the human touch
□ c. Reliability on technology
□ d. Lack of technical training
□ e. Unfriendly or complicated learning system
□ f. Little or no focus on quality
□ g. Poor awareness on the benefits of e-Learning
□ h. Security issues
□ i. Other (please specify)

3. Risk assessment model for assessing the risk of e-Learning environment

Q12. As part of your role, do you identify critical risk exposures when using e-Learning applications or in the e-Learning environment?

□ a. Yes
□ b. No
□ c. I do not know

Q13. Do you know if your institution /or company has a risk management policy in place?

□ Yes
□ No
□ I do not know

Q14. Which of the following security risks is your institution /or company exposed to? (Select all that apply)

□ a. Malicious damage (e.g. corruption of data and software)
□ b. Unauthorised access (e.g. unauthorised viewing)
□ c. Accidental error/human carelessness (e.g. computer operator error)
□ d. Mechanical failure (e.g. hardware/software error damages file)
□ e. Online Fraud
□ f. Invasion or loss of privacy/confidentiality
□ g. Other (Please write in)

Q15. How do you assess the risks involved in using the e-Learning environment? (Select all that apply)

□ a. Seek opinion of those already using the applications
□ b. Seek the services of a risk consultant
□ c. Carefully analyse precedents to improve forecasting
□ d. Look at all of the things that could go wrong and develop a contingency plan in case they do
□ e. Read newspapers, trade journals, regulations etc. to help you make an informed decision
□ f. Other (Please write in)

Q16. Do you quantify risks in terms of their impact and probability?

□ a. Yes
□ b. No
□ c. I do not know

Q17. Do you have a risk assessment / or management framework for your e-Learning applications?

□ a. Yes
□ b. No (Go to Q.19)
□ c. I do not know

Q18. Are there any risk improvement measures in place?

□ a. Yes
□ b. No
□ c. I do not know

If yes, please specify:

□

Q19. Is there any system for identifying risks?

□ a. Yes
□ b. No
□ c. I do not know

If yes, please specify:

□

Q20. Which of the following methods are used for managing the e-Learning risks within your institution /or company? (Select all that apply)

□ a. Take out an insurance policy
□ b. Absorb risk
□ c. Forecast and plan ahead
□ d. Agree a fixed fee with a risk management company
□ e. Make a contingency plan
□ f. Use experienced and reliable dealers
□ g. Line up a secondary source of supply
□ h. Take a risk
□ i. Identify and value all assets at risk
□ j. Put safeguards and controls (e.g. policies, procedures etc) in place
□ k. Assess risk periodically
□ l. Other (Please write in)

□

Q21. Do you consider your e-Learning environment safe?

□ a. Yes
□ b. No
□ c. I do not know

Q22. Are remote users authenticated before being allowed to connect to internal networks and systems?

□ a. Yes
□ b. No
□ c. I do not know

4. Contents and Usage

Q23. What is the proportion of the overall content of your module that is available on the course website?

□ a. 100%

□ b. 75%

□ c. 50%

□ d. 25%

□ e. Unsure

Q24. How often do you access the course materials?

□ a. Daily

□ b. Once a week

□ c. Twice a week

□ d. Once a month

Q25. How would you rate the ease of using the e-Learning system in your institution /or company?

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
User friendly	○	○	○	○	○

Q26. What is your experience of using the following tools in your e-Learning environment?

	Very useful	Useful	Not useful	Do not know	Cannot remember
a. Discussion	○	○	○	○	○
b. Lecture slides	○	○	○	○	○
c. Lecture notes	○	○	○	○	○
d. Past question paper	○	○	○	○	○
e. Class experiment	○	○	○	○	○
f. Timetable	○	○	○	○	○
g. Self assessment	○	○	○	○	○
h. Interactive lectures	○	○	○	○	○
i. News and alerts	○	○	○	○	○
j. Announcements	○	○	○	○	○
l. Charts	○	○	○	○	○
m. Who’s online	○	○	○	○	○

Q27. Do you trust that resources available online (lecture notes, tutorials, workshops, etc.) are a good substitute for the actual classroom learning?

□ Yes
□ No (please specify)

5. Security Measures

Q28. In your opinion is e-Learning security an important issue for your institution /or company?

□ Yes
□ No
□ Unsure

Q29. Do you know that the learning system adopted by your institution is internet based and can be prone to intrusion by attackers?

□ Yes
□ No
□ Unsure

30. Do you know if security policy in relation to e-Learning has been implemented in your institution / or company?
(If your answer is “No” or “Unsure”, please go to Q.33)

□ Yes
□ No
□ Unsure

Q31. Is your institution /or company's security and privacy policy available to the general public?

□ Yes
□ No
□ I do not know

If No, please specify why:

Q32. Which of the following measures is required for login?

□ a. Password
□ b. Firewall
□ c. Public Key Encryption
□ d. Private Key Encryption
□ e. Digital Signature
□ f. Biometrics
□ g. Others (please specify)

	Never	Rarely	Sometimes	Usually	Every time
Q33. Do you share your login details with anyone?	○	○	○	○	○

Q34. Are you required to use any other authentication method apart from the password?

□ Yes
□ No
□ Unsure

If yes, please specify:

Q35. Are you able to access resources /or services off-campus?

□ Yes
□ No

If yes, please specify:

Q36. Which of the following risks do you think the e-Learning system is prone to?

□ a. Hacking
□ b. Identity Theft
□ c. Fraud
□ d. Denial of Service
□ e. Unauthorised modification of course contents
□ f. Others (please specify)

6. Social Awareness

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Q37. It is often said that absolute security is unattainable. To what extent do you agree with this statement?	○	○	○	○	○

Q38. What should be done to address the issue of potential loss of confidence by users in the e-Learning environment?
(If you have no comment(s), please write in ‘None’)

Q39. Please specify any problems you might have encountered that are not covered in the above sections (e.g. not having a suitable security or risk assessment procedure in your institution / or company).
(If you have no comment(s), please write in ‘None’)

Q40. Would you like to participate in the follow-up studies (e.g. case study /or interview)?

□ **Yes**

□ **No**

I promise not to use the details or individual responses in any publications. I also promise not to pass your details to any other researchers or organisations. All the information provided will be protected under the ‘Data Protection Act 1998’.

This research is focused on the ‘Security Issues in e-Learning’. I would be happy to send you a free copy via e-mail. (Please tick all that is appropriate to your business operations)

□ **Outcomes of this questionnaire research**

□ **Summary of PhD outcomes**

□ **All of the above**

□ **None**

Email

Thank you very much for completing this research survey.

Submit

Appendix B: DEACCF Validation Questionnaire

DEACCF Validation Questionnaire

In the understanding that you are a busy professional, 5 minutes of your time will be well-appreciated in helping us to validate our proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF). On completion of this study, a summary of findings will be sent to you. Neither confidential information nor any company's details are being sought in the questionnaire. Instead, the aim is to validate our Framework.

Please note that this is an academic research survey, and NOT a marketing or product survey. The DEACCF is attached to the back to the back of this questionnaire.

1. **Are you E-Learning developer?**

   □ **Yes** *(If "Yes", go to Questions 2 and 3)*

   □ **No** *(If "No", you do not need to continue)*

2. **Do you integrate security platform to the E-Learning system that your organisation for the clients?**

   □ **Yes**

   □ **No**

3. **Will you consider using DEACCF to develop client's E-Learning system?**

   □ **Yes**

   □ **No** (*If "No", please explain why you / or your organisation will not adopt DEACCF)*

Thank you very much for completing the questionnaire!

Appendix C: Email Template to E-Learning Developers and DEACCF Description

Date: XX XXX XXXX

Name: XXXXXX XXXXXXXXXX
Address: XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX

Subject: Validation of the Dynamic E-Learning Access Control and Copyright Framework (DEACCF)

Dear E-Learning Developer,

It was a great pleasure talking to you on the phone and I am extremely grateful for your voluntary willingness to participate in validating the proposed DECAFF. With your expertise, I am humbly asking you to answer the following survey questions that will help in validating the attached framework.

Once again, many thanks for accepting to participate in validating our proposed framework.

Galina Akmayeva

Note:
Confidentiality of Research Records:

- Only the researcher has access to contact information and responses;
- Your personal identifying information will only be used to contact you.

Potential Risks and Discomforts:

- No physical, social or economic risks are posed to participants.
- Participating in the study will not affect your current legal status, services provided or status.

If you have any further questions relating to the proposed framework, please feel free to contact me via email at galina.akmayeva@brunel.ac.uk or Skype: Gakmayeva74

Proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF)

We have proposed the Dynamic E-Learning Access Control and Copyright Framework (DEACCF) as a result of the security weaknesses found in the most widely used E-Learning models. It was noted during our investigation that none of the existing models has multi-factor authentication method. Therefore, we have integrated the latter to our framework.

The proposed DEACCF has three Phases (see Figure 1). The significant contribution of DEACCF is based on the unique selections of the security elements. From the user's access point the system initiated five combinations of security:

- Biometrics =>Digital Signature => QR Code =>House/Mobile Phone number
- Biometrics => Pattern Recognition => QR Code =>House/Mobile Phone number
- Username / Password => Home/Mobile Phone number => QR Code =>Biometrics
- Digital Signature => QR Code => Home/Mobile Phone number => Biometrics
- Pattern Recognition => QR Code => Home/Mobile Phone number => Biometrics

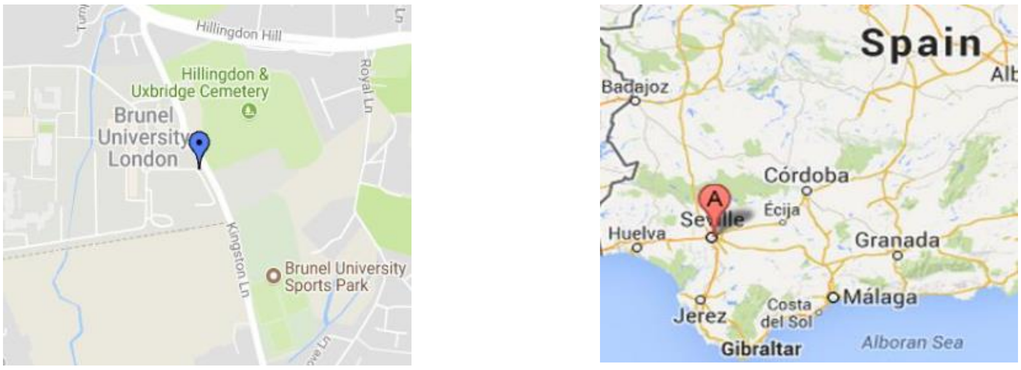
The above attributes can be prompted in any order. However, the only element that will be in a consistent state is the biometrics enrolment status. The user access point requires multi-dependence attributes as detailed above.

PHASE 1

The single-factor authentication will be incorporated into Phase 1 of the proposed DEACCF. The user signs in using Username and the system prompts for Password. The user will be asked to enrol his/her device(s). User can only enrol 4 devices (mobile phone, android, laptop and desktop, or any applicable devices) using device identifier that enables each of the device's serial number / or manufacturer's identification number to be recognised.

- Google Locator

The Google locator identifier will deter the security breach by not allowing unauthorised user to login to the E-Learning system. It gives the specific location of the user (see Figure 2(a) and (b)).



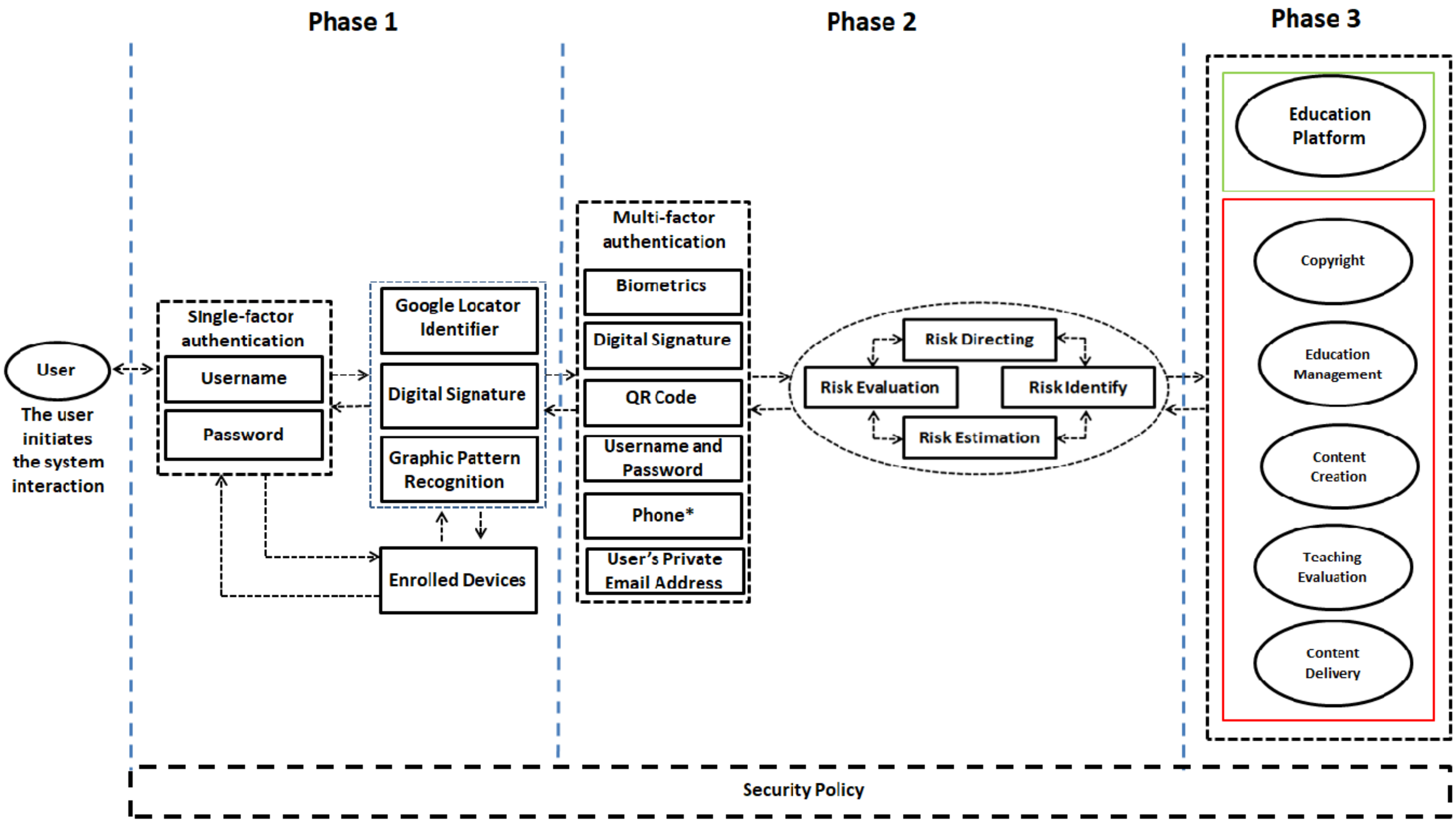
(a)

User lives in London, but currently on holidays in Spain

(b)

User's current location is showing in Google map

Figure 2 (a) and (b). Google User's Specific Location



Phone* (House and/or Mobile Phone Numbers)

Figure 53. Proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF)

The latter will also enhance Copyright Policy. Each time a user is changing location (traveling abroad /or moving to a new location), as long as the address on the system is different, the user will not be able to login. Therefore, the user must update the address on the system 24 hours before any changes can be effective.

- Digital Signature and Graphic Pattern Recognition

The digital signature and pattern recognition separately give additional security level and also provide a unique element to the public and private keys that are related. The public key will encrypt the signature and only the corresponding private key can be used to decrypt it. The digital signature uses two keys instead of one key (symmetric encryption). It is virtually impossible to deduce the private key if you know the public key (see Figure 3).

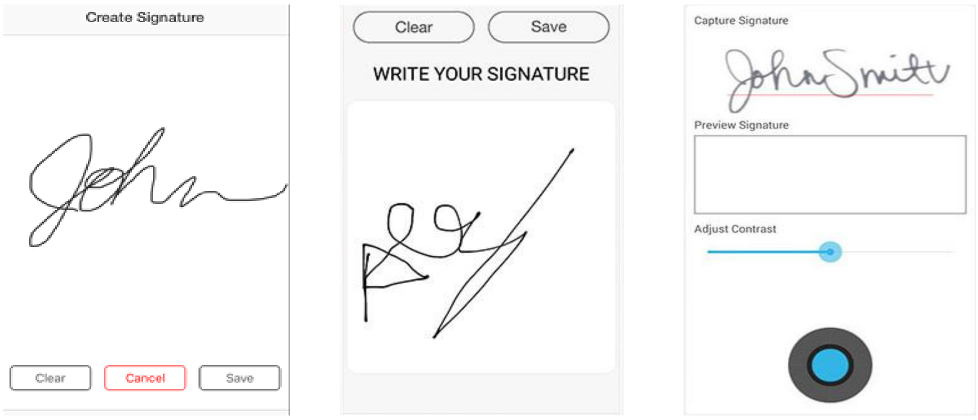


Figure 3. Screen Shot of Digital Signatures

The built-in graphic pattern lock tool is useful for adding an extra layer of security to Phase 1 but cannot be used at the same time with the digital signature. The pattern is recorded in a more recognised way to identify any misappropriate space or line (see Figure 4).

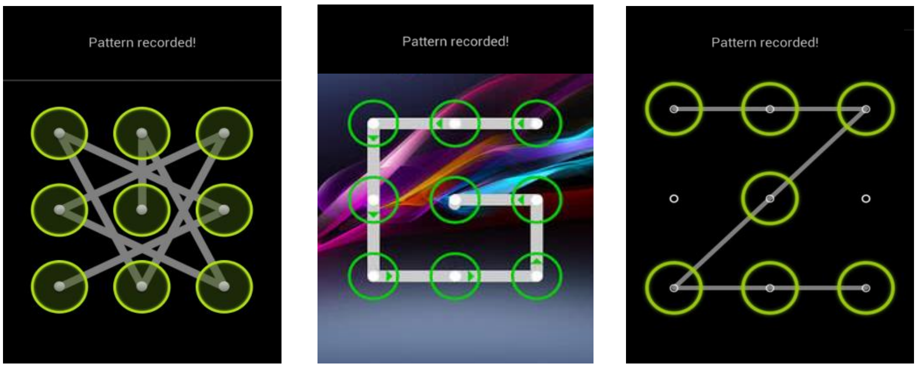


Figure 4. Screen Shot of Graphic Pattern Recognition

User can use the pattern recognition to secure the interaction between their device and the Phase 2.

PHASE 2

The Phase 2 is based on the multi-factor authentication process of matching the attributes that the users provided during the enrolment. The matching attributes initiate combinations of elements and their attributes which are processed in order to verify the user.

- Biometrics

The biometrics technology, that has been integrated to the DEACCF, has the ultimate form of electronics security verification of physical attribute of a person. We combined biometrics with other verification attribute to, so that the user's specific location and identity can be verified at a given time during and after interacting with the system (Phase 2 of DEACCF).

- Quick Response (QR) Code

The QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used.

Figure 5. QR Code

The QR Code provides the following:

1. High Capacity Encoding of Data
2. Small Printout Size
3. Kanji and Kana Capability
4. Dirt and Damage Resistant
5. Readable from any direction in 360 degrees.
6. Structured Appending Feature

The user will download the QR code reader on his/her mobile phone that will be used to scan the QR code on his/her student's ID card (see Figures 5 and 6).

The student's identity needs to be verified in line with the other sets of Access Control attributes as outlined above.

- House and/or Mobile Phone

The DEACCF requires the user to type or input their house (landline) /or mobile phone number that was used during the enrolment. However, if the user enrolled iOS /or Android tablets, they will not be asked to input phone number. The house (landline) /or mobile phone number are equally important when authenticating the user's legitimate access control.

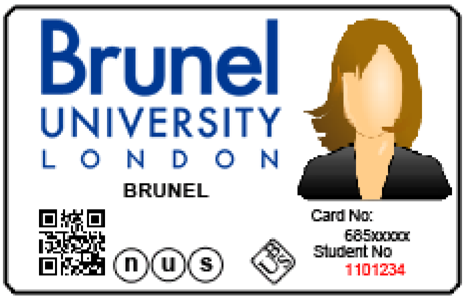


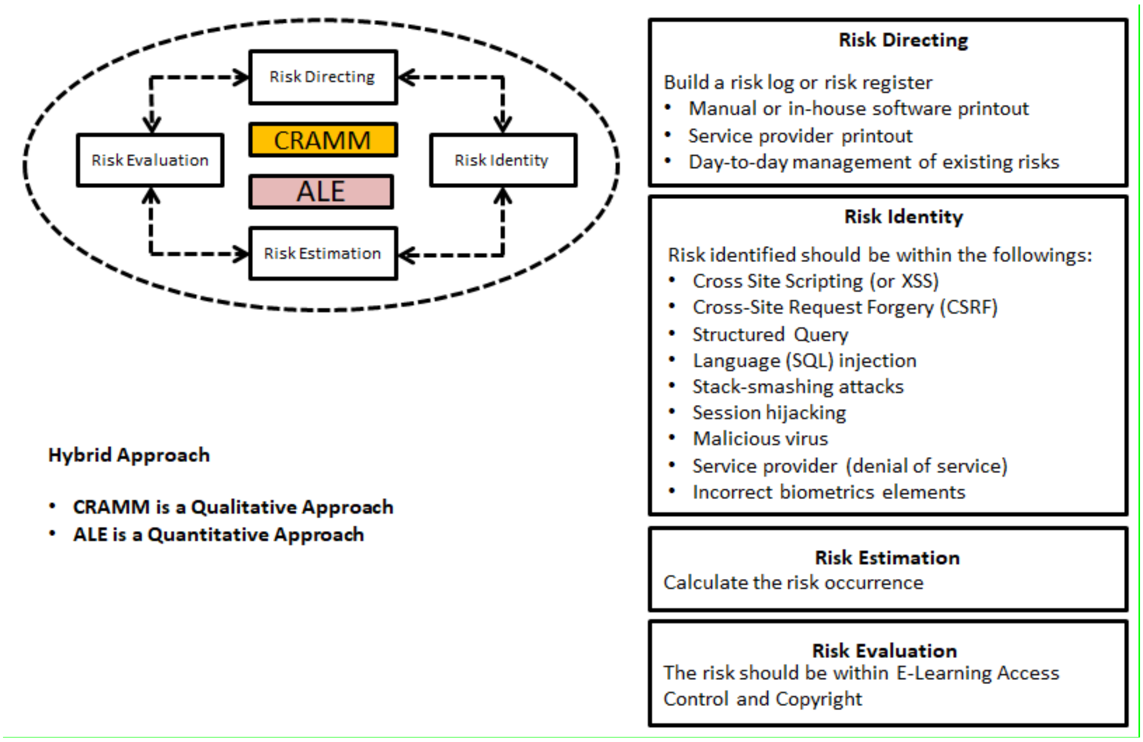
Figure 6. Student's ID with QR Code

- User's Private Email Address

The user's private email address is used for further verification. The user will be instructed to login to the private email address provided in order to click on the verification code. The latter will accept the verification code. All other things being equal, the Access Control set of attributes should and must be verified without any error.

- Risk Assessment Process

The risks of any security breaches while trying to login are mitigated by the risk assessment process as shown in the DEACCF (see Figure 1). We used Hybrid Approach Risk Assessment Model which is based on Quantitative and Qualitative Approaches (see Figure 7).



Hybrid Approach

- **CRAMM is a Qualitative Approach**
- **ALE is a Quantitative Approach**

Risk Directing

Build a risk log or risk register

- Manual or in-house software printout
- Service provider printout
- Day-to-day management of existing risks

Risk Identity

Risk identified should be within the followings:

- Cross Site Scripting (or XSS)
- Cross-Site Request Forgery (CSRF)
- Structured Query
- Language (SQL) injection
- Stack-smashing attacks
- Session hijacking
- Malicious virus
- Service provider (denial of service)
- Incorrect biometrics elements

Risk Estimation

Calculate the risk occurrence

Risk Evaluation

The risk should be within E-Learning Access Control and Copyright

Figure 7. E-Learning Security Threats Risk Assessment Model

An appropriate risk assessment approach is in place to tabulate associated numerical security risk to financial /or cost implication for the institution /or organisation.

PHASE 3

Finally, the Phase 3 is the final stage of the DEACCF, which consists of the "Education Platform" that processes the data generated from E-Learning materials (see Figure 1 - Proposed Dynamic E-Learning Access Control and Copyright Framework (DEACCF)). The Copyright elements relating to the proposed framework is based on trust from all parties involved in the development and the dissemination of the E-Learning materials.

Note:

If you have any further questions relating to the proposed framework, please feel free to contact me via email at galina.akmayeva@brunel.ac.uk or Skype: Gakmayeva74

References

Abernathy, D., (1999). Thinking Outside the Evaluation Box. Training and Development Magazine. February, 53(2), pp18-23 [online] Available: http://web.ebscohost.com/ehost (Accessed 12 December 2010).

Acunetix, (2018). "SQL Injection (SQLi)". https://www.acunetix.com/websitesecurity/sql-injection/. (Access date: 8 March, 2018)

Adelabu, O.A., Adu, E.O., Adjogri, S.J., (2014). The Availability and Utilization of E-Learning Infrastructures for Teaching and Learning. Mediterranean Journal of Social Sciences, Vol.5, No.23.

Adeoye, B.F., (2010). "Socio-Cultural Dimensions of E-Learning Systems", Transformative Learning and Online Education: Aesthetics, Dimensions and Concepts.

Adetoba B. T., Awodele O., Kuyoro S. O., (2016), E-learning security issues and challenges: A review, Journal of Scientific Research and Studies Vol. 3(5), pp. 96-100, May, 2016.

Adobe, (2017). Digital signatures explained.https://acrobat.adobe.com/uk/en/sign/ capabilities/digital-signatures-faq.html. (Access date: 11 August 2017).

Agrawal, M., (2015). Implementing eLearning: Know The Challenges And Opportunities, eLearning Industry, https://elearningindustry.com/implementing-elearning-know-challenges -opportunities, (Access date: 12 February, 2016).

Aïmeur, E., Hage, H., Mani Onana, F.S., (2008). Anonymous Credentials for Privacy-Preserving E-learning. 2008 International MCETECH Conference on e-Technologies.

Aladwan, A.A., Shamroukh, R.M., Aladwan, A.A., (2012). A Novel Study of Biometric Speaker Identification Using Neural Networks and Multi-Level Wavelet Decomposition, World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 2.

Alexander, S., (2001). E-Learning developments and experiences. Education and Training, Bradford 43(4-5).

Alkharang, M. M., Ghinea, G., (2013). E-learning in Higher Educational Institutions in Kuwait: Experiences and Challenges. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.4, 2013.

Al-Jumeily, D., Williams, D., Hussain, A. and Griffiths, P., (2010). Can We Truly Learn from A Cloud Or Is It Just A Lot of Thunder? 2010 Developments in E-systems Engineering.

Alotaiby, F. T., Chen, J. X., (2004). A model for team-based access control (TMAC 2004). International Conference on Information Technology: Coding and Computing.

Al-Khouri, A. M., and Bal, J., (2007). Digital identities and the promise of the technology trio: PKI, smart cards, and biometrics. Journal of Computer Science, 3(6), 361.

Altinkemer, K., Wang, T., (2011). Cost and benefit analysis of authentication systems, journal decision support systems, vol. 51, issue 3.

Alwi, N. H. M., Fan, I. S., (2010). E-learning and information security management. International Journal of Digital Society (IJDS), 1(2).

Amant, K., (2005). Distance education in a global age: a perspective for internationalizing online learning communities. SIGGROUP Bulletin, ACM Press, 25, 12-19.

Anastasia, (2015). “Computer-Based Training”, Cleverism, https://www.cleverism.com/ lexicon/computer-based-training/, (Access date: 2 March 2016).

Anderson, T., and Elloumi, F., (2004). Theory and practice of online learning, Athabasca, Canada: Athabasca University.

Apampa, K. M., G. B. Wills, et al., (2008). Electronic integrity issues in e-assessment security. ICALT 2008: The 8th IEEE International Conference on Advanced Learning. Spain.

Apampa, K. M., Wills, G., & Argles, D. (2010). User security issues in summative e-assessment security. International Journal of Digital Society, 1(2), 135-147.

Arakelyan, V.A., (2013). Vulnerable Security Problems in Learning Management System (LMS) Moodle. Mathematical Problems of Computer Science 39.

Ardagna, C., Cremonini, M., Damiani, E., di Vimercati, S., and Samarati, P., (2006). Supporting location-based conditions in access control policies.

Association of Modern Technologies Professionals, (2018). Cloud Computing, Corporate Management, http://www.itinfo.am/eng/cloud-computing (Access Date: 2 January, 2018).

Aviation Industry CBT Committee (AICC), (2008). www.aicc.org, (Access date: 2 April, 2016).

Bača, M., Grd, P., and Fotak, T., (2012). Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics. INTECH.

Baier, D., Bertocci, V., Brown, K., Woloski, M., Pace, E., (2010). A Guide to Claims-Based Identity and Access Control, Microsoft.

Babbie, E., (2010). The practice of social research. Belmont, CA: Wadsworth. (301.072_BAB).

Bandara, I., Ioras, F., Maher, K., (2014). Cyber Security Concerns in E-Learning Education. Proceedings of ICERI2014 Conference 17th-19th November 2014, Seville, Spain. ISBN: 978-84-617-2884-0.

Bao, C., Castresana, J. M., (2012). Virtual Learning Environments: Concepts, Methodologies, Tools and Applications, edited by Management Association, Information Resources.

Barik N., Karforma, S., (2012). Risks and remedies in e-learning system. Int. J. Netw. Secur. Appl. 4(1):51-59.

Bashah Mat Ali, A., Yaseen Ibrahim Shakhatreh, A., Syazwan Abdullah, M., Alostad, J., (2011). “SQL-injection vulnerability scanning tool for automatic creation of SQL-injection attacks”, Procedia Computer Science, Vol. 3.

Baukes, M., (2018). Everybody Knows: How Knowledge-Based Authentication Died. Forbes.https://www.forbes.com/sites/forbestechcouncil/2018/01/22/everybody-knows-how-knowledge-based-authentication-died/#7a81b9344eee. (Access date: 7 May, 2018)

Baxter I., Hughes, C., and Tight, M., (1988), ‘How to research’, Open University Press.

BBC, (2017). Copyright Aware. http://www.bbc.co.uk/copyrightaware/what-is. (Access date: 1 March 2017).

Becta, (2006). E-portfolios – Process Model. Coventry: Becta.partners.becta.org.uk/ index.php?section=pv&&catcode=_pv_ep_02&rid=13627, (Access date: 13 April 2016).

Benson, R., Brack, C., (2010). Online learning and assessment in higher education. Oxford, UK: Chandos Publishing.

Berge, Z., (1998). Guiding principles in Web-based instructional design. Education Media International, Vol. 35No.(2).

Best College Reviews, (2015), 50 Top Online Learning Sites, https://www.bestcollege reviews.org/50-top-online-learning-sites/ (Access Date: 28, Feburary 2015).

Bhargav-Spantzel, A., Squicciarini, A., Bertino, E., (2007). Privacy Preserving Multi-Factor Authentication with Biometrics. Proceedings of the second ACM workshop on digital identity management.

BioLink, (2017). "Fingerprint Recognition", Advanced Biometric Solutions http://www.biolinksolutions.com/technology/fingerprint.php, (Access date: 4 December 2016).

Bishop, M., (2004). Introduction to Computer Security. Published by Addison-Wesley Professional.

Blackboard Privacy Policy, (1997-2015). http://www.blackboard.com/footer/privacy-policy.aspx.

Blackboard Inc., (2017). "Blackboard Delivers Worldwide Growth". PR Newswire. https://www.prnewswire.com/news-releases/blackboard-delivers-worldwide-growth-300398129.html. (Access date: 23 April, 2018)

Blaze, M., Feigenbaum, J., and Ioannidis, J., (1999). The Keynote Trust-Management System Version 2.

Boehm, P., Justice, M., & Weeks, S., (2009). Promoting academic integrity in higher education. The Community College Enterprise, 15(1), 45-61.

Bogdan, R.C., Biklin S. K., (1998). Qualitative research for education: An introduction to theory and methods. (3rd ed.) Boston: Allyn and Bacon.

Bolle, R., Connell, J., Pankanti, S., Ratha, N., and Senior, A., (2003). Guide to Biometrics Springer Professional Computing. New York Inc.: Springer-Verlag.

Bonderud, D. (2016), The Move to Multifactor Authentication: Are Passwords Past Their Prime? https://securityintelligence.com/news/the-move-to-multifactor-authentication-are-passwords-past-their-prime/ (Access date: 27 December 2016).

Botsios, S., Georgiou, D., (2010). "Standardization in User Modeling and Learning Objects Retrieval: Recent Contributions", Monitoring and Assessment in Online Collaborative Environments: Emergent Computational Technologies for E-Learning Support. IGI Global.

Brainard, A., Juels, R.L., Rivest, M. Szydlo, M., and Yung, M., (2006). Fourth-factor authentication: Somebody you know. In ACM CCS, 168–178.

Brandon, B., (2013). IMS Global Learning Consortium: Interoperability Standards for Education, (Access date: 6 February, 2016).

Bryman, A., and Bell, E., (2011). Business Research Methods (3 ed.). Oxford: Oxford University Press.

Butson, R., (2003). “Learning objects: weapons of mass instruction”. British Journal of Educational Technology, Vol 34, No. 5, pp667-269.

Burns, R.B., (1997). Introduction to research methods. (3rd ed.) Australia: Longman.

Buss, D., (2005). “Two Factor, Too Tough?”, Securities Industries News, June 6.
Carliner, S., (1999). Overview of online learning. Amherst, MA: Human Resource Development Press.

Carliner, S., (2004). "An Overview of Online Learning", 2 edition, HRD PRESS, INC.

Casebourne, I., (2017), How does blended learning compare to elearning and face-to-face training? Learning Technologies Group plc, https://leolearning.com/2017/11/blended-learning-elearning-face-face-training/ (Access Date: 3 November, 2017).

Cedefop, (2001). E-Learning and training in Europe, A survey into the use of E-Learning in training and professional evelopment in the European Union, Cedefop Reference series, Luxembourg: Office for Official Publications of the European Communities.

Choi, C., Choi, J., Ko, B., Oh, K., Kim, P., (2014). Ontology-based access control model for security policy reasoning in cloud computing. Journal of Super Computing. 67(3), 711-722.

Chikh, A., (2014). A general model of learning design objects, Journal of King Saud University - Computer and Information Sciences, Vol. 26, Issue 1.

Childs, J. (2000). "The Future for E-Learning", "t" Magazine, June.

Christova, A., Mihai, A., (2011) ‘Teaching European studies: A blended learning approach’, International Journal of Emerging Technologies in Learning (iJET) 6(4).

Ciobanu, C.-L., Ciobanu, N.-M., (2012). E-learning Security Vulnerabilities, Elsevier.

Clark, C.R., 2005, Catalogue. Cortez, CO: Clark Training and Consulting.

Clinch, J., (2009). ITIL V3 and Information Security, White paper.

Clouse, L.D., (2003). Virtual Border Customs: Prevention of International Online Music Piracy Within the EverEvolving Technological Landscape, ValpoScholar, Volume 38 Number 1, https://scholar.valpo.edu/cgi/viewcontent.cgi?article=1336&context=vulr (Access Date: 6 October, 2016.

Collis, B., and Moonen, J., (2001). Flexible learning in a digital world: experiences and expectations, London: Kogan Page.

Collis, J. and Hussey, R., (2009). Business Research: A practical guide for undergraduate and postgraduate students, 3rd Ed. England: Palgrave Macmillan.

Connolly, T. and Begg, C., (2005). Database Systems; A practical Approach to Design, Implementation and Management: Fourth Edition. Harlow: Pearson.

Conrad, K., (2000). TrainingLinks, Instructional design for web-based training, Amherst: HRD Press.

Conrad, Kerri A. and TrainingLink, (2000). Instructional Design for Web-based Training. Amherst, MA: HRD Press.

Corominas, J., (1987). Breve diccionario etimológico de la Lengua Castellana. Madrid: Gredos.

Costinela – Luminitaa, C.D., (2011). Information security in E-learning Platforms. Procedia Social and Behavioral Sciences 15 (2011), 2689-2693.

Coulson, C., (2016). Configuring Forms Based Authentication in SharePoint 2016 – Part 4 – Adding Users to the Membership Database, Chris Coulson's Developer Notes, https://blogs.visigo.com/chriscoulson/configuring-forms-based-authentication-in-sharepint-2016-part-4-adding-users-to-the-membership-database/. (Access date: 14 January, 2017).

Couros, A., (2010). Developing personal learning networks for open and social learning. Emerging technologies in distance education. Edmonton, AB: AU Press.

Covington, M. J., Long, W., Srinivasan, S., Dev, A. K., Ahamad, M., and Abowd, G. D., (2001). Securing context-aware applications using environment roles.

Craver, S., Memon, N., Yeo, B., Young, M., (1997). "On the invertibility of invisible watermarking techniques", Proc. Of the IEEE Int. Conf. On Image Processing 1997, Vol. 1.

Creswell, J.W., (2011). Research Design. Fourth Edition. Pearson.

Creswell J.W., Plano Clark V.L., (2011). Designing and conducting mixed methods research. 2nd ed. Thousand Oaks, CA: Sage.

CSO Magazine, (2011). US Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University, Deloitte: 2011 Cybersecurity Watch Survey. Tech. rep.

Davis, P., (2004). VPN/Security. Cisco Technology Enabling E-Learning, Cisco Systems, Inc.

Dekker, M., (2009). Flexible Access Control for Dynamic Collaborative Environments.
PhD thesis, University of Twente.

Denning, D. E. and MacDoran, P. F., (1996). "Location-based authentication: Grounding cyberspace for better security," Computer Fraud and Security, vol. 1996.

Denso Wave, (2011). The Inventor of QR Code, "QR Code features", http://www.qrcode.com/en/, Access date: 15 September 2016.

Deutsch, W., (2017). Learn how to secure your building and property, The Balance, https://www.thebalance.com/how-to-secure-your-building-and-property-394590, (Access date: 8 November, 2017)

Devine, S., (2013). "The Rise of Mobile Technology in Higher Ed", Huffpost, https://www.huffingtonpost.com/sean-devine/the-rise-of-mobile-techno_b_3466751.html, (Access date: 4 April 2016).

Dick, M., Sheard, J., Bareiss, C., Carter, J., Joyce, D., Harding, T., and Laxer, C., (2002). Reports from ITiCSE on innovation and technology in computer science education. ACM SIGCSE bulletin working group, 35(2).

Dillenbourg, P., 1999, What do you mean by “collaborative learning”? In P. Dillenbourg (Ed.) Collaborative learning: cognitive and computational approaches. Amsterdam: Pergamon.

Dittmann, J., (2000). “Digital Wasserzeichen,” Springer, Berlin.

DocuSign, (2017). Understanding digital signatures. https://www.docusign.co.uk/how-it-works/electronic-signature/digital-signature/digital-signature-faq. (Access date: 12 September 2017).

Dublin, L., (2004). “The nine myths of E-Learning implementation: ensuring the real return on your E-Learning investment.” Industrial and Commercial Training, Vol 36, No.7.

Duncan, C., Ekmekcioglu, C., (2003). Digital Libraries and Repositories, in A. Littlejohn (Ed.) Reusing Online Resources: a sustainable approach to e-learning. London: Kogan Page.

Earle, R., (Ed.), 2000, Standards for the accreditation of programs in educational communications and technology. Bloomington, IN: Association for Educational Communication and Technology.

Easton, G., (2010). “Critical Realism in Case Study Research,” Industrial Marketing Management (39).

Editvu-SECURITY, (2002). Your content is well-protected, Online, Available at www.editvu.com/security.html (Access date: 12 November 2014).

Educause, (2010). 7 Things You Should Know About LMS Alternatives, https://net.educause.edu/ir/library/pdf/ELI7062.pdf, (Access date: 2 March 2015).

Educause, (2017). E-Learning. https://library.educause.edu/topics/teaching-and-learning/e-learning, (Access date: 7 December 2017).

Electronic Collaboration: a Practical Guide for Educators, (1999). A joint production of Northeast and Islands Regional Educational Laboratory at Brown University.

El-Khatib, K., Korba, L., Xu, Y., and Yee, G., (2003). "Privacy and Security in E-Learning." International Journal of Distance Education 1(4).

Elrod, R., (2005). “Two-factor Authentication”, East Carolina University.

Encyclopaedia Britannica, (2015). Security and protection system: Personal and property protection. http://www.britannica.com/technology/security-and-protection-system. (Access date: 2 February 2015).

Erden, M., (2018). Advantages and Disadvantages of Biometric Authentication. SESTEK. http://www.sestek.com/2016/11/advantages-disadvantages-biometric-authentication/. (Access date: 7 March, 2018)

Ettinger, A. Holton, V., and Blass, E., (2005). “E-learner experiences: learning from the pioneers.” Industrial and Commercial Training, Vol 37, No. 6, pp286-290.

European Commission, (2005). The elearningeuropa.info website, European Communities. http://www.elearningeuropa.info (Access Date: 25 December, 2011).

Evered, R. and Reis Louis, M., (2001). Alternative Perspectives in the Organizational Sciences: ‘Inquiry from the Inside’ And ‘Inquiry from the Outside’, in Academy of Management Review, Vol. 6, No. 3.

Ezhilmaran, D., Adhiyaman, M., (2017). A review study on latent fingerprint recognition techniques. Journal of Information and Optimization Sciences, Vol. 38, Issue 3-4.

EY, (2016). Risk? Integrity? What’s accelerating your growth?, EYGM Ltd.

Farrell, G., (1999). The Development of Virtual Education: A global perspective: A study of current trends in the virtual delivery of education, conducted with funding provided by the Department for International Development, London, U.K., Publisher: Commonwealth of Learning.

Federal Trade Commission, (2015). Start with security, A Guide for Business.

Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., (2016). Authentication Protocols for Internet of Things: A Comprehensive Survey.

Fulantelli, G., Gentile, M., Taibi, D., Allegra, M., (2008). The Open Learning Object model to promote Open Educational Resources. Open University, UK.

Ferraiolo, D., Kuhn, D., and Chandramouli, R., (2003). Role Based Access Control. Artech House.

Fishman, T.D., Sledge, L., (2014). Reimagining higher education: How colleges, universities, businesses, and governments can prepare for a new age of lifelong learning, Deloitte Insights, https://www2.deloitte.com/insights/us/en/industry/public-sector/reimagining-higher-ededucation.html (Access Date: 13 May, 2016).

Floyd, C., Schultz, T., and Fulton, S., (2012). Security vulnerabilities in the open source Moodle eLearning system. In Proceedings of the 16th Colloquium for Information System Security Systems Security Education. Lake Buena Vista, Florida. ISBN 1-933510-95-1.

Fontana, J. (2009). Nursing faculty experiences of students' academic dishonesty. Journal of Nursing Education, 48(4), 181-5.

Fordham IT, (2016). Multi-Factor Authentication at Fordham is a Necessary Good, https://itnews.blog.fordham.edu/?p=823. (Access date: 14 January 2017).

Friedman, J., (2018). Study: More Students Are Enrolling in Online Courses. https://www.usnews.com/higher-education/online-education/articles/2018-01-11/study-more-students-are-enrolling-in-online-courses. (Access date: 23 May, 2018).

Fritz, G., Seifert, C. and Paletta, L., (2006). A mobile vision system for urban detection with informative local descriptors, Proceedings of International Conference on Computer Vision Systems, 2006.

Fry, K., (2001). “E-Learning markets and providers: some issues and prospects.” Education and Training, Vol 43, No. 4/5.

Fujitsu, (2014). Fujitsu innovates PalmSecure multi-factor authentication device for the Hyperconnected World. http://www.fujitsu.com/uk/news/pr/fs-20141118-1.html (Access date: 12 June 2016).

Fuller, R. M., Vician, C., Brown, S. A., (2006). E-learning and individual characteristics: the role of computer anxiety and communication apprehension. Journal of Computer Information Systems, 46, 4.

Furnell, S., (2007). An assessment of Website password practices. Computers & Security, 26(78), 445-451.

Gaebel, M., Kupriyanova, V., Morais, R., Colucci, E., (2014). E-Learning in European Higher Education Institutions. Results Of A Mapping Survey Conducted In October-December 2013.

Gao, Q., (2012). Using IP addresses as assisting tools to identify collusions. International Journal of Business, Humanities and Technology, 2(1), 70-75.

Garrison, D. R. and Anderson, T., 2003, E-Learning in the 21st century: A framework for research and practice. London: RoutledgeFalmer.

Gaya, J., (2013). Pros and Cons Of Campus Learning Vs Online Learning, ELearning Industry.https://elearningindustry.com/pros-and-cons-of-campus-learning-vs-online-learning, (Access date: 8 November 2016).

Ginzburg, L., Sitar, P., Kelly Flanagin, G., (2006). User Authentication System and Method. (NJ). USA.

Goodyear, P., (2001). Effective networked learning in higher education: notes and guidelines. See: http://www.csalt.lancs.ac.uk/jisc/guidelines_final.doc. (Access date: 25 May, 2014).

Graf, F., (2002). "Providing Security for E-Learning", Computers and Graphics, vol. 26, no. 2.

Great Britain, (2018). Data Protection Act. London: Stationery Office.

Gregor, S., Jones, D., (2007). The Anatomy of a Design Theory. Journal of the Association for Information Systems 8, 5, 312-335.

Guiller, J., Bell, D., (2011). Who-Wants-An-Interative-Lecture: Embedding Use of Personal Response Systems to Enhance the Student Learning Experience, Final Report to the Higher Education Psychology Network, Departmental Teaching Enhancement Scheme, https://www.heacademy.ac.uk/system/files/guiller_and_bell_final_report.pdf, (Access date: 12 June, 2015).

Gupta, P., (2016). Some interesting statistics and facts on blended learning you must know, EdTechReview,http://edtechreview.in/data-statistics/2506-blended-learning-in-the-class-room-statistics-research, (Access date: 13 May 2017).

Hacker Bulletin, (2016). Different Types of Cryptographic Attacks. http://www.hackerbulletin.com/types-cryptographic-attacks/. (Access date: 13 March, 2017).

Hall, B., (1997). The Web-based Training Cookbook. Published by John Wiley and Sons Inc.

Heimdal Security, (2017). Session Hijacking Takes Control of Your Accounts. Here’s How. https://heimdalsecurity.com/blog/session-hijacking/. (Access date: 1 November, 2017).

Hanyan, H., (2012). Research of E-commerce Security Strategies Based on Cloud Computing Platform. 1487-1493. 10.1007/978-94-007-2169-2_176.
1997

Hartung, F. and Kutter, M., (1999). Multimedia watermarking techniques. Proceedings of the IEEE 87(7).

Hasan, S. H., Alghazzawi, D. M., Zafar, A., (2016). E-Learning Systems and their Security. Journal of Management Research Report.

Hay Newman, L., (2017). Security news this week: A one-stop guide to zero-day exploits. WIRED. https://www.wired.com/2017/03/security-news-week-everything-know-zero-day-exploits/, (Access date: 3 December, 2017).

Hawker, A., (2000). Security and Control in Information Systems, A guide for business and accounting.

Heinrich, E., (2005). Exploring the Use of the IMS Learning Design Specification for Facilitating Formative Assessment. From Proceeding (495) Education and Technology.

HESA, Data Collection, (2017). https://www.hesa.ac.uk/collection/c16051/coverage. (Access date: 3 March 2018).

Hevner, A. R., March, S. T., Park, J., and Ram, S., (2004). "Design Science in Information Systems Research." Management Information Systems Quarterly, 28(1), 75-106.

Hill, P., (2011) "Analysis of Blackboard Response to Recent Disclosure of Security Vulnerabilities" http://www.deltainitiative.com/bloggers/author-philhill/analysis-of-blackboard-response-to-recent-disclosure-of-securityvulnerabilities, (Access date: 4 March 2014).

Himberg, J., Korpiaho, K., Mannila, H., Tikanmaki, J. and Toivonen, H. T. T., (2001). Time series segmentation for context recognition in mobile devices, Proceedings of International Conference on Data Mining, 2001.

Hoffman, K.E., (2014). Less than zero: Zero-day vulnerabilities. SC Media, https://www.scmagazine.com/less-than-zero-zero-day-vulnerabilities/article/540109/, (Access date: 4 April 2015).

Holloway, S., (2010), Cloud Computing: What is it really? Bloor Research, https://www.bloorresearch.com/2010/03/cloud-computing-what-is-it-really/, (Access date: 15 November, 2014).

Horton, W., (2000). Designing web-based training. New York: Wiley.

Howell, J., and Wei, J., (2010). Value increasing model in commercial e-banking. The Journal of Computer Information Systems, 51(1).

Huang, J., Nicol, D.M., (2012). Trust mechanisms for cloud computing. Springer Open Journal of Cloud Computing. August 2(9).

Hugl, U., (2005). Tech-developments and possible influences on learning processes and functioning in the future. Journal of American Academy of Business, 6(2).

Hussein, H.A., (2015), E-learning, Online Learning and Distance Learning: Are they the same?, IT e-Magazine, Issue 5, March, http://lfu.edu.krd/item/issue05/issue_Elearning.php (Access Date: 16 May, 2016).

Hwang, Y., (2016). Understanding social influence theory and personal goals in e-learning, Information Development 2016, Vol. 32(3).

Hyder, K., Kwinn, A., Miazga, R., Murray, M., Edited by Brandon, B., (2007). Synchronous E-Learning, Published by The eLearning Guild.

Identity Automation, (2018). Risk-Based Authentication.https://www.identityautomation.com/iam-platform/rapididentityidentity-access-management/multi-factor-authentication/risk-based-authentication/. (Access date: 8 May, 2018).

IDology, (2014). Knowledge Based Authentication (KBA) – Out-of-Wallet Questions. https://www.idology.com/knowledge-based-authentication/knowledge-based-authentication-kba. (Access date: 2 January 2016).

Imperva, (2018). Cross Site Request Forgery (CSRF) Attack.

https://www.incapsula.com/web-application-security/csrf-cross-site-request-forgery.html. (Access date: 12 January, 2018).

IMS Global Learning Consortium, (2002). IMS learning design: best practice and implementation guide. See: http://www.imsglobal.org/learningdesign/ldv1p0pd/imsld_ bestv1p0pd.html (Access Date: 8 March 2012).

Infosec Institute, (2018). Access Control: Models and Methods. https://resources.infosecinstitute.com/access-control-models-and-methods/#gref. (Access date: 1 June 2018).

Ingle, D., Meshram, B.B., (2012). Hybrid Analysis and Design Model for Building Web Information. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3.

ISO/IEC 21827, (2002). Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM).

ISO/IEC 15408, (2004). Common Criteria for Information Technology Security Evaluation, Version 2.2.

ISO/IEC 27001, (2013). Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (ISO), https://www.iso.org/standard/54534.html, (Access date: 16 February 2015).

ITU CCITT: Security Architectures for Open Systems Interconnection for CCITT Applications {Recommendation X.800. International Telecommunication Union (ITU), The international telegraph and telephone consultative committee (CCITT), Geneva, 1991.

Jabade, V., Gengaje, S., (2016). Modelling of geometric attacks for digital image watermarking. International journal of innovations in engineering research and technology [IJIERT], ISSN: 2394-3696 VOLUME 3, ISSUE 3, March, 2016.

Jaros, D., Kuchta, R., (2010). “New Location Based Authentication Techniques in the Access Management”, Wireless and Mobile Communications (ICWMC) 6th International Conference, 2010, pp. 426 – 430.

Jing, Z., Dong-Dai, L., Guo-Cui, M., (2011). “A universal distributed model for password cracking”, pp. 955-960.

Johnson, R.B., Onwuegbuzie, A., Turner, L.A., (2007). Toward a Definition of Mixed Methods Research, Journal of Mixed Methods Research, DOI: 10.1177/155869806298224.

Johnson M., (2013). Cyber Crime, Security and Digital Intelligence Book, Gower Publishing, Ltd.

Jolliffe, A., Ritter, J., Stevens, D., (2001). The online learning handbook: developing and using webbased learning. London: Kogan Page.

Jonassen, D.H., Davidson, M., Dollins, M., Campbell, J. and Bannan Haag, B., 1995, Constructivism and computer-mediated communication in distance education. The American Journal of Distance Education 9(2).

Jones, L.A., Anton, A.I., and Earp, J.B., (2007) Towards understanding user perceptions of authentication technologies. ACM Workshop on Privacy in Electric Society.

Jordan, J., (2015). Campuses deploy multi-factor via higher ed ‘cohortium’. SecureIDNews. https://www.secureidnews.com/news-item/campuses-deploy-multi-factor-via-higher-ed-cohortium/. (Access date: 4 May 2016).

Jørstad, I. and Thanh, D. V., (2007). The mobile phone as authentication token, Telenor ASA.

Jung, B., Han, I. and Lee, S. (2001). "Security Threats to Internet: A Korean Multi-Industry Investigation", Information and Management, vol. 38, no. 8.

Kadansky, M., (2010). Data Security: How can I protect my paper records?, Personalized Computer Services, http://www.kadansky.com/files/newsletters/2010/2010_06_28.html, (Access date: 11 March, 2017).

Kajava, J., and Savola, R., (2005). Weak Signals in Information Security Management. In: Proceedings of the International Conference on Computational Intelligence and Security (CIS) 2005, Part II, Xi’an, China, December 15-19, 2005. Springer.

Kambourakis, G., Damopoulos, D., (2013). A Competent Post-Authentication and Non-Repudiation Biometric-based Scheme for M-Learning. Proceedings of the 10th IASTED International Conference on Web-based Education (WBE 2013).

Kamoun, A., Tazi, S., (2014). “A semantic role-based access control for intra and inter-organization collaboration”, in Proceedings of IEEE Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Parma, Italy,pp. 86-91.

Kane, E., and O’Reilly-de Brun, M., (2001). Doing your Own Research, Marion Boyars Publishers.

Karp, A.H., Haury, H., and Davis, M. H., (2009). From ABAC to ZBAC: the evolution of access control models. In tech. report, HP Labs.

Karvonen, K., (1999). Creating Trust. Proceedings of hte Fourth Nordic Workshop on Secure IT Systems Nordsec '99), Kista, Sweden.

Kay R., (2005). Biometric Authentication. ComputerWorld, http://www.computerworld. com/article/2556908/security0/biometric-authentication.html, (Access date: 5 February 2016).

Kearsley, G., (2000). “Online Education: Learning and Teaching in Cyberspace”. Belmont, CA: Wadsworth.

Keegan, D., (2000), Distance training: taking stock at a time of change. London: Routledge Falmer.

Keith, M., Shao, B. and Steinbart. P. J., (2007). The usability of passphrases for authentication: An empirical field study. International journal of human-computer studies, 65(1):17–28.

Kelly T., (2005). “The business case for E-learning” published by Cisco Press.

Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Lopez, J., (2012). “Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms”.

Kerr, L., Alves-Foss, J., (2016). Combining Mandatory and Attribute-Based Access Control. 2016 49th Hawaii International Conference on System Sciences (HICSS). Electronic ISBN: 978-0-7695-5670-3

Ketel, M., (2014). E-learning in a cloud computing environment. Conference Proceedings - IEEE SOUTHEASTCON. 1-2. 10.1109/SECON.2014.6950728.

King, C.G., Guyette, R. W., and Piotrowski, C., (2009). Online exams and cheating: An empirical analysis of business students’ views. The journal of Educators Online, 6(1).

Klein, A., (2002). "Cross Site Scripting Explained". Sanctum Security Group. https://crypto.stanford.edu/cs155/papers/CSS.pdf (Access date: 13 December 2014).

Knowledgepool, (2000). http://www.knowledgepool.com/our_core_competencies/online_blended_learning/home.html, (Access date: 2 January 2012).

Koufman-Frederick, A., Lillie, M., Pattison-Gordon, L., Lynn Watt, D., Carter, R., (1999), Electronic Collaboration: A Practical Guide for Educators, The Education Alliance Brown University.

Kuhn, R., Coyne, E. J., and Weil, T. R., (2010). Adding Attributes to Role Based Access Control. Technical report, IEEE Computer Society.

Kumar Singh, S., (2016). Cloud Computing: Comparative Study Own Server vs Cloud Server. 590-598. 10.1142/9789814704830_0056.

Kumar, G., and Chelikani, A., (2011), Analysis of security issues in cloud based e-learning, University of Borås Sweden, https://pdfs.semanticscholar.org/3e1d/97c698f79ded58b 9dc980b4fdb3c7debc022.pdf (Access Date: 15 June, 2016).

Kumar, S. and Dutta, K., (2011). Investigation on Security in LMS MOODLE. nternational Journal of Information Technology and Knowledge Management January-June 2011, Volume 4, No. 1.

Kutter, M., Voloshynovskiy, S., Herrigel, A., (2000). “Watermark copy attack,” In Ping Wah Wong and Edward J. Delp eds., IS&T/SPIE's 12th Annual Symposium, Electronic Imaging 2000: Security and Watermarking of Multimedia Content II, Vol. 3971 of SPIE Proceedings, San Jose, California USA.

Lape, L.G., (1992). Ownership of Copyrightable Works of University Professors: The Interplay between the Copyright Act and University Copyright Policies. Vill. Law Review, 37(2).

Laurillard, D., 2002, New technologies, students and the curriculum: the impact of communications and information technology on higher education, in Scott, P (ed) Higher education re-formed. London: Palmer Press.

Lay, S., (2015). The Uncanny Valley Effect. Doctoral thesis. Open University, UK

Lessard, D., Lucea, D., (2009). Embracing risk as a core competence: The case of CEMEX, Journal of International Management, Vol. 15, Issue 3.

Levy, D., (2011). Lessons learned from participating in a connectivist massive online open course (MOOC). In Y. Eshet-Alkalai, A. Caspi, S. Eden, N. Geri & Y. Yair (eds.), Proceedings of the Chais conference on instructional technologies research: Learning in the technological era, (pp. 31-36).http://www.openu.ac.il/research_center/chais2011/download/f-levyd94_eng .pdf. (Access date: 12 November, 2016).

Li, J., (2010). Study on the Development of Mobile Learning Promoted by Cloud Computing. IEEE.

Li, J., (2010). Robust image watermarking scheme against geometric attacks using a computer-generated hologram. US National Library of Medicine National Institutes of Health.https://www.ncbi.nlm.nih.gov/pubmed/21068862, (Access date: 12 January, 2016).

Lin, E.T., Cook, G. W., Salama, P. and Delp, E.J., (2001). An overview of security issues in streaming video. Proceedings of the International Conference on Information Technology: Coding and Computing, Las Vegas, 2-4 April.

Lin, C., Wu, M., Bloom, J., Cox, I., Miller, M., Lui, Y., (2001). Rotation, scale and translation resilient watermarking for images, IEEE Trans. Image Process. 10 (5).

Lipka, S. (2009, April). Colleges sharpen tactics for resolving academic-integrity cases. The Chronicle of Higher Education, 55(31), A20.
Liu, R., Tan, T., (2002). An SVD-based watermarking scheme for protecting rightful ownership. IEEE Transactions on Multimedia.

Lo, N.W., Guo, T.C.Y.M.H., (2015). An Attribute-Role Based Access Control Mechanism for Multi-tenancy Cloud Environment. Wireless Pers Commun, Springer Science+Business Media, New York.

Logan, D., (2001). E-Learning in the knowledge age. Gartner Symposium Itxpo 2001. 30 July –1 August 2001, Johannesburg, South Africa.

LTSC (Learning Technology Standards Committee), (2000). Learning technology Standards committee web pages. See: http://www.ltsc.ieee.org/, (Access date: 20 June 2014).

Lynch, M., (2016), Cyberlearning vs. Elearning – Is there a difference?, http://www.thetech-edvocate.org/cyberlearning-vs-elearning-difference/ (Access Date: 12 December, 2016).

Ma, Y., and Feng, J., (2011). Evaluating usability of three authentication methods in web based application. Ninth International Conference on Software Engineering Research, Management and Application. August 2011. Baltimore, MD.

MacDonald, C. J., Stodel, E. J., Farres, L. G., Breithaupt, K, Gabriel, M. A., (2001). The demand-driven learning model: a framework for web-based learning. The Inernet and Higher Education 4.

Maiwald, E., (2003). Network Security a Beginner’s Guide, 2 Ed., McGraw-Hill/Osborne, 2003.

Malik, A. K., Mateen, A., Abbasi, M.A., Malik A. A., (2017). A Comparison of Collaborative Access Control Models. International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 3.

March, S.T., Smith, G.F., (1995). Design and natural science research on information technology. Decision Support Systems 15, 251- 266.

Marcinko, D.E., Hetico, H.R., (2016). Risk Management, Liability Insurance, and Asset Protection Strategies for Doctors and Advisors. CRC Press.

Marshall E-Learning Consultancy, (2018). "Off the shelf". https://marshallelearning.com/e-learning-courses/information-security/. (Access date: 7 May, 2018).

Martin, F., Parker, M. A., (2014). "Use of Synchronous Virtual Classrooms: Why, Who, and How?", MERLOT Journal of Online Learning and Teaching. Vol. 10, No. 2, June.

Mcclure, S., Scambray, J., Kurtz, G., (2012). Hacking Exposed: Network Security Secrets and Solutions, 7 Ed., McGraw-Hill/Osborne.

Malouff, J. M. and Sims, R. L., (1996). Applying an employee-motivation model to prevent student plagiarism Journal of Education for Business 72.

Marforio, C., Karapanos, N., Soriente, Kostiainen, K., and Capkun, S., (2014). Smartphones as practical and secure location verification tokens for payments. In Proceedings of the Network and Distributed System Security Symposium (NDSS).

Martin, F. and Connor, M., (2017), Using Blended Learning to Aid Law and Business Students’ Understanding of Taxation Law Problems, Journal of the Australasian Tax Teachers Association Vol.12 No.1.

Mayes, T. and de Freitas, S. (2004) Review of e-learning theories, frameworks and models. London: Joint Information Systems Committee. http://www.jisc.ac.uk/whatwedo/ programmes/elearningpedagogy/outcomes.aspx, (Access date: 4 February, 2016).

McGinity, M., (2005). Staying connected: Let your fingers do the talking. Communications of the ACM, 48(1), 21-23.

Mesec, B., (1998). Uvod v kvalitativno raziskovanje v socialnem delu. Ljubljana: Visoka šola za socialno delo.

Mehrabian, A., (1971). Silent Messages, Wadsworth Publishing Company.

Meinecke, J., Gaedke, M., Majer, F., Brändle, A., (2007). Modeling and Managing Federated Web-based Systems. Conference: Conference: 3rd International Conference on Web Information Systems and Technologies (WEBIST).

Mertens, D.M., (2005). Research methods in education and psychology: Integrating diversity with quantitative and qualitative approaches. (2nd ed.) Thousand Oaks: Sage.

Micallef, N., Just, M., Baillie, L., Halvey, M., Guene, H., (2015). Why Aren'T Users Using Protection? InvestigatingtheUsabilityofSmartphoneLocking.InProceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15).ACM, New York, NY, USA, 284–294.

Microsoft: Dynamic System Initiative Roadmap - Web Site. (2003).

Miller, D. E., Kunce, J. T., (1973). Prediction and statistical overkill revisited, Measurement and Evaluation in Guidance.

Miller, B., (2017). The Big Benefits of Blended Learning, LEO Learning, https://leolearning.com/2017/07/big-benefits-blended-learning/, (Access date: 12 August, 2017).

Miločević, M., (2013). Information security in e-learning: The matter of quality. Preceedings, eLearning conference, (September): 26–27.

Miločević, M., Miločević, D., Sādhanā, D., (2016). Defining the e-learner's security profile: Towards awareness improvement, Indian Academy of Sciences.

Mimoso, M., (2016). MiniUPnP Vulnerability Clears Way for Stack Smashing Attack. https://threatpost.com/miniupnp-vulnerability-clears-way-for-stack-smashing-attack/116030/. (Access date: 1 January, 2017).

Mishra, S., 2002, Building online learning environments. (Online). Commonwealth of Learning, Available: http://www.col.org/Knowledge/ks_online.htm (Accessed on 26 September 2003).

Mishra, A., Mishra, D., (2011). E-learning experience at various universities: Academics perspective, Tehnicki Vjesnik 18.

Mohamed, T.S., (2014). Security of Multifactor Authentication Model to Improve Authentication Systems. Information and Knowledge Managment Journal, Vol.4 Issue 6.

Moonian, O., Cheerkoot-Jalima, S., Nagowaha, S. D., Khedoa, K. K., Doomuna, R., and Cadersaiba, Z., (2008). Hcrbac an access control system for collaborative context-aware healthcare services in mauritius. Healthcare Informatics in Developing Countries.

Morrison, N., (2014). Distance learning is now open to all thanks to the Internet, The Telegraph,http://www.telegraph.co.uk/education/expateducation/11231600/Distance-learning-is-now-open-to-all-thanks-to-the-Internet.html, (Access date: 17 November 2015).

Morrison, C., Secker, J., (2015). Copyright Literacy in the UK: a survey of librarians and other cultural heritage sector professionals, Library and Information Research, 39 (121), 75–97.

Muramatsu, B., (2008). IEEE 1484.20.1, Data Model for Reusable Competency Definitions Published. IEEE Learning Technology Standards Committee.

National Research Council, (2011). "Learning Science Through Computer Games and Simulations". Committee on Science Learning: Computer Games, Simulations, and Education, Margaret A. Honey and Margaret L. Hilton, Eds. Board on Science Education, Division of Behavioral and Social Sciences and Education. Washington, DC: The National Academies Press.

Naude, E., and Hoerne, T., (2006). Cheating or collaborative work: Does it pay? Issues in Informing Science and Information Technology.

Ndume, V., Tilya, F.N., and Twaakyondo, H., (2008). Challenges of adaptive eLearning at higher learning institutions: A case study in Tanzania. International Journal of Computing and ICT Research, 2(1).

Neuman, W. L., (2003). Social Research Methods: Qualitative and Quantitative Approaches. Boston, Pearson Education Inc.

Nicol D., Sanders W. H., Trivedi K. S., (2004). Model-Based Evaluation: From Dependability to Security. In: IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, January/March.

Nielsen, J., (1999). Designing Web Usability: The Practice of Simplicity. New Riders Publishing Thousand Oaks, CA, USA.

Nishanth, N., Babu, S., (2014). Sequence Number Alteration by Logical Transformation (SALT): A Novel Method for Defending Session Hijacking Attack in Mobile Ad hoc Network. International Journal of Computer and Communication Engineering, Vol. 3, No. 5.

NIST, (2017). Access Control Policy and Implementation Guides, Computer Security Resource Centre, https://csrc.nist.gov/Projects/Access-Control-Policy-and-Implementation-Guides, (Access date: 3 March 2017).

Nunamaker, J.F., Jr., Chen, M., and Purdin, T.D.M., (1991). Systems Development in Information Systems Research. Journal of Management Information Systems 7, 3, 89-106.

Odhiambo, O. and Acosta, F.R., (2009). An E valuation of the Usability and Interactivity of e-Learning Platforms Used In Kenyan Universities. In T. Bastiaens, J. Dron & C. Xin (Eds.), Proceedings of E-Learn 2009--World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, Vancouver, Canada: Association for the Advancement of Computing in Education (AACE), https://www.learntechlib.org/p/32589/ (Access Date: 3 April, 2017).

O'Gorman, L., (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12).

Oluoch, S.J., (2014). Improving Password Security Using Location–Based Intelligence. International Journal of Scientific and Research Publications.

Oppliger, R., Pernul, G., Strauss, C., (2004). Using Attribute Certificates to Implement Role-based Authorization and Access Controls.

O'Ruanaidh, J., Pun, T., (1998). Rotation, scale, and translation invariant digital image watermarking, Signal Process. 66 (3).

OWASP, Foundation, (2011). "OWASP Testing Guide", 2008. V3.0. http://www.owasp.org/images/ 5/56/OWASP_Testing_Guide_v3.pdf, October.

Pappas, C., (2013). Top 10 e-Learning Statistics for 2014 Infographic. http://elearningindustry.com/top-10-e-learning-statistics-for-2014-you-need-to-know. (Access date: 26 February 2014).

Pappas, C., (2015). "Summative Assessment In eLearning: What eLearning Professionals Should Know", eLearning Industry, https://elearningindustry.com/summative-assessment-in-elearning-what-elearning-professionals-should-know, (Access date: 18 November 2016).

Park, F., Gangakhedkar, C., and Traynor, P., (2009). Leveraging cellular infrastructure to improve fraud prevention. In Proceedings of the Annual Computer Security Applications Conference (ACSAC).

Patas, J., Milicevic, D., Goeken, M., (2011). "Enhancing Design Science through Empirical Knowledge: Framework and Application", in H. Jain, A. Sinha, and P. Vitharana, (eds.), Service-Oriented Perspectives in Design Science Research. Springer Berlin / Heidelberg, pp. 32-46.

Peffers, K., Tuunanen, T., Rothenberger, M. A., Chatterjee, S., (2008). "A Design Science Research Methodology for Information Systems Research." Journal of Management Information Systems, 24(3), 34.

Peterson, R., (2000). Constructing Effective Questionnaires, Sage Publications.

Pfleeger, S. L., Cunningham, R. K., (2010). Why Measuring Security is Hard. IEEE Computer and Reliability Societies.

Piirainen, K. A., Briggs, R. O., (2011). "Design Theory in Practice – Making Design Science Research More Transparent ", Service-Oriented Perspectives in Design Science Research. Springer, pp. 47-61.

Pila, J., (2010). Who owns the intellectual property rights in academic work? European Intellectual Property Review.

Pimlott, A., Kiselyov, O., (2006). Soutei, a Logic-Based Trust-Management System. In FLOPS 2006, 8th International Symposium on Functional and Logic Programming, pages 130–145, Fuji-Susono, Japan. Also in Springer's Lecture Notes in Computer Science.

Prins, M., Abma, J., (2010). Security research Blackboard Academic Suite, https://www.online24.nl/blackboard-security-research, (Access date: 6 November 2015).

Polsani, P. R., (2003). 'Use and abuse of reusable learning objects', http://www.jodl.ecs.s oton.ac.uk/Articles/v03/i04/Polsani/. (Access date: 20 June 2014).

Pop, A., (2015), Study Portals Online Courses, https://www.distancelearningportal.com/ articles/294/10-top-uk-universities-ideal-for-distance-learning.html, (Access Date: 22, February 2015).

Pop, A., (2016). Blended Learning, E-Learning and Online Learning: What's Important?, Distance Learning Portal, https://www.distancelearningportal.com/articles/269/blended-learning-e-learning-and-online-learning-whats-important.html (Access Date: 13 February, 2017).

Pop, A. (2017). 10 U.S. Universities Offering Top Distance Education. https://www.mastersportal.com/articles/1307/10-us-universities-offering-top-distance-education.html. (Access date: 18 April, 2018).

Rabai, L.B.A., Rjaibi, N., Ben Aissa, A., (2012). Quantifying Security Threats for E-learning Systems.

Rahmatian, A., (2014). Make the butterflies fly in formation? Management of copyright created by academics in UK universities. Legal Studies, 34(4).

Rajesh, (2017). What is Biometrics Authentication, Learning and Experience, learning.maxtech4u.com/what-is-biometrics-authentication/, (Access date: 12 December, 2017).

Rana, M., (2011). Types of Access Control Mechanisms. Tech Mahindra. https://www.techmahindra.com/sites/blogs/types_of_access_control_mechanisms.aspx. (Access control: 1 June, 2016).

Rana, H., Rajiv, Lal, M., (2014). E-learning: Issues and Challenges. International Journal of Computer Applications. 97. 20-24. 10.5120/17004-7154.

Ramim, M., (2006). Securing E-Learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University. Journal of Cases on Information Technology (JCIT).

Rao, N. M., Sasidhar, C. and Kumar, V. S., (2010). Cloud Computing Through Mobile-Learning. Computing, 1.

Remenyi, D., Williams, B., Money, A. and Swartz, E., (2003). Doing research in business and management: An introduction to process and method, London, SAGE Publications.

Renner, J., (2016). Copyright, eLearning, And Creativity. E-Learning Industry. https://elearningindustry.com/copyright-elearning-and-creativity. (Access date: 2 February, 2018).

Research Advisor (2006). Sample size table. http://www.research-advisors.com/tools/SampleSize.htm. (Access date: 26 April, 2015)

Research and Markets, (2017). Global E-Learning Market Analysis & Trends - Industry Forecast to 2025, https://www.researchandmarkets.com/research/qgq5vf/global_elearning (Access date: 24 December 2017).

Richards, C., (2002). Distance education, on-campus learning, and E-Learning convergences: an Australian exploration. International Journal on E-Learning July-September.

Rittenhouse, R. G., Chaudry, J. A. and Lee, M., (2013). “Security in Graphical Authentication”, International Journal of Security and Its Applications, Vol. 7, No. 3.

Rodchua, S., Yiadom-Boakye, G., and Woolsey, R., (2011). Student verification system for online assessments: Bolstering quality and integrity of distance learning. Journal of Industrial Technology, 27(3).

Rogers, J., Usher, A., Kaznowska, E., (2011) The state of e-learning in Canadian universities, 2011: If students are digital natives, why don't they like e-learning? Toronto: Higher Education Strategy Associates.

Rossman, G.B., and Rallis, S.F., (2011). Learning in the Field: An Introduction to Qualitative Research, Sage Publications, Inc. Third Edition.

RSA, (2017). Risk-Based Authentication, RSA Information Design and Development, https://community.rsa.com/docs/DOC-77387, (Access date: 7 May, 2018).

Ruzic-Dimitrijevic, L., Dakic, J., (2014). The risk management in higher education institutions, Online Journal of Applied Knowledge Management, Vol. 2, Issue 1.

Sagar, K., Waghmare, V., (2016) “Measuring the Security and Reliability of Authentication of Social Networking Sites”, Proceedings of International Conference on Communication, Computing and Virtualization (ICCCV), 79, 668-674. https://doi.org/10.1016/j.procs.2016. 03.085.

Salah, A. A., Alpaydin, E. and Akarun, L., (2002). A selective attention-based method for visual pattern recognition with application to handwritten digit recognition and face recognition, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, 2002.

Sammour, G. N., (2013). Elearning Systems Based on the Semantic Web, iJET International Journal of Emerging Technologies in Learning, http://www.online-journals.org/index.php/i-jet/article/viewFile/2/10 (Access Date: 10 December, 2017).

Sanders, E. S., and Thiagarajan, S., (2001). Performance intervention maps. Alexandria, VA: American Society for Training and Development.

Sandhu, R., Samarati, P., (1994). Access Control: Principles and Practice. Communication Magazine, IEEE, 32 Issue 9.

Sandhu, R., Coyne, E., Feinstein, H., and Youman, C., (1996). Role Based Access Control Models, Computer-Los Alamitos.

Sandhu, R., (1998). Role Based Access Control, Advances in Computers.

Sandhu, R., (2001). Future Directions in Role Based Access Control. Information Assurance in Computer Networks, Lecture Notes on Computer Networks, Volume 2052.

Sanka S., Hota C., Rajarajan M., (2010) Secure Data Access in Cloud Computing. In: Proceedings of the IEEE 4th International Conference on Internet Multimedia Services Architecture and Applications (IMSAA).

Santelli, S., (2016). "The Future Of [Virtual] Education", D!gitalist Magazine, https://www.digitalistmag.com/industries/higher-education-and-research/2014/07/30/future-virtual-education-01257501, (Access date: 12 November 2015).

Saunders, M., Lewis, P., Thornhill, A., (2012). Research methods for business students. 6th Ed, London: Pearson.

Saxena, R., (2004). Security and online content management: balancing access and security, 12th biennial VALA conference and exhibition, Melbourne, Australia, Victorian Association for Library Automation (VALA).

Scientific American. (2013), "Big Data Goes to School". Special report "Learning in the digital age". www.hep.fsu.edu/~wahl/artic/SA/mag/2013/201308.pdf. (Access date: 13 November 2015)

Schneier, B., (2003). Beyond fear: Thinking sensibly about security in an uncertain world, New York: Springer-Verlag.

Secker, J., Morrison, C.M., (2016). Copyright education and training. In: J. Secker & C.M. Morrison (Eds.), Copyright education and training. (pp. 211-238). London, UK: Facet Publishing. ISBN 1783300604

SecureAuth, (2015). SecureAuth Survey: 66% of Cybersecurity Professionals Moving Beyond Traditional Passwords.https://www.secureauth.com/company/newsroom/ secureauth-survey-66-cybersecurity-professionals-moving-beyond-traditional. (Access date: 23 March 2016).

Security Industry Authority, (2016). "British Standards e-Learning", https://www.sia.homeoffice.gov.uk/Pages/acs-elearning.aspx. (Access date: 2 February, 2017).

Şerb, A., Defta, L.L., Iacob, N.M., and Apetrei, M.C., (2013). Information Security Management in E-Learning, Knowledge horizons, Volume 5, No. 2. http://orizonturi.ucdc.ro/arhiva/2013_khe_2_pdf/khe_vol_5_iss_2_55to59.pdf (Access Date: 26 July, 2017).

Shar, L.K., Tan, H.B.K., (2012). “Auditing the XSS defence features implemented in web application programs” Software, IET on 2012 (Volume: 6, Issue: 4) Page(s): 377 – 390.

Sharma, S., (2005). "Location Based Authentication" University of New Orleans Theses and Dissertations. Paper 141.

Sheppard, N., (2014). Digital copyright protection – some success, but mostly failure. Phys.org. (Access date: 2 March, 2016).

Sherekar, S., Thakare, V.M., Jain, S., (2011). Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks. International Journal Of Computer Science And Applications Vol. 4, No. 2, June July 2011.

Siciliano, R., (2017). The Definition of Financial Identity Theft and Affinity Fraud, The Balance, https://www.thebalance.com/identity-theft-and-affinity-fraud-4117147, (Access date: 12 July, 2017).

Sinclair, J., Joy, M., Yin-Kim Yau, J., and Hagan, S., (2013). A Practice-Oriented Review of Learning Objects. IEEE Transactions on Learning Technologies, Vol. 6, No. 2.

Singh, P., Chadha, R.S., (2013). A Survey of Digital Watermarking Techniques, Applications and Attacks. International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9.

Soler-Labajos, N., and Jiménez-Zarco, A.I., (2016), E-Commerce: The Effect of the Internet and Marketing Evolution, Encyclopedia of E-Commerce Development, Implementation, and Management.

Song, K. S., Lee, S. M., & Nam, S., (2013a). Cognitive biometrics application for e-learning security enhancement. International Journal of Bio-Science and Bio-Technology, 5(3), 143-152.

Song, K., Lee, S.M., Nam, S.C. (2013b). Combined biometrics for e-learning security. ISA 2-13, ASTL, 21, 247-251.

SOPHOS, (2017). "How to configure One-time Password (OTP)", https://community. sophos.com/kb/en-us/120324, (Access date: 3 March 2017).

Special Report, (2013). Learning in the digital age. Scientific America, August.

Srivastava, A., (2018), eLearning Companies in the UK, http://www.learninglight.com/ elearning-companies-uk/. (Access date: 12 January 2018).

Stokes, S., (2014). The future of digital copyright. Inflaw. http://www.infolaw.co.uk/ newsletter/2014/05/the-future-of-digital-copyright/. (Access date: 1 March, 2016).

Strauss, N., (2011). Anything but academic: how Copyright's work-for-hire doctrine affects professors, graduate students, and K-12 teachers in the information age. Richmond Journal of Law and Technology, XVIII, 1.

Su, S.Y.W. and Lee, G., (2004). A Web-Services-based E-Learning Infrastructure for Managing Virtual E-Learning Communities. In J. Nall & R. Robson (Eds.), Proceedings of E-Learn 2004-World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, Association for the Advancement of Computing in Education (AACE), https://www.learntechlib.org/p/11096/ (Access Date: 14 January, 2018).

Summers, W.C., and Bosworth, E., (2004). Password policy: the good, the bad, and the ugly. ACM International Conference Proceeding Series; Proceedings of the Winter International Symposium on Information and Communication Technologies 58.

Sun, S.T., Hawkey, K., Beznosov, K., (2012). "Systematically breaking and fixing OpenID security: Formal analysis, semi-automated empirical evaluation, and practical countermeasures", Computers and Security, Vol. 31, No. 4.

Sunesh, H.K., (2011). Watermark Attacks and Applications in Watermarking. National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC), Proceedings published in International Journal of Computer Applications.

Takeda, H., Veerkamp, P., Tomiyama, T., and Yoshikawam, H., (1990). "Modeling Design Processes." AI Magazine Winter: 37–48.

TCSEC, Trusted Computer System Evaluation Criteria, "Orange Book", (1985). U.S. Department of Defense Standard, DoD 5200.28-std

The Learning Group, (2003). About E-Learning: Benefits, The Learning Group, http://www.learngroup.com.au (Access Date: 15 July, 2011).

The next web (TNW), (2015). How to Increase App Security Through Mobile Phone Authentication.https://thenextweb.com/future-of-communications/2015/03/16/increasing-application-security-with-mobile-phone-authentication/. (Access date: 16 November 2016).

The Phantoms, (2017). Introduce About Cross-Site Scripting (XSS). https://th3phantoms.blogspot.co.uk/2017/02/introduce-about-XSS.html, (Access date: 7 November, 2017).

The Scottish Government, (2016). Enhancing Learning And Teaching Through The Use Of Digital Technology, https://beta.gov.scot/publications/. (Access date: 8 March, 2017).

The University of British Columbia, (2010). Digital Learning and Curriculum (DLC), http://www.dlc-ubc.ca/dlc1/?q=node/306 (Access Date: 17 May, 2017).

Thomas, R. and Sandhu, R., (1998). Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. Database Security.

ThreatMetrix, (2017). Risk-Based Authentication and The Evolving Threat of Account Takeover. https://www.threatmetrix.com/digital-identity-blog/risk-based-authentication/risk-based-authentication-evolving-threat-account-takeover/, (Access date: 8 September, 2017)

Timewade - Infinite possibilities, Cloud Computing, What is “Cloud Computing” and how does this affect my business?, http://www.timewade.com/services/cloud-computing (Access Date: 5 January, 2018).

Towhidi, F., Manaf, A. A., Daud, S. M. and Lashkari, A. H., (2011). “The Knowledge Based Authentication Attacks”, in World Congress in Computer Science.

Trend Micro, (2017). Ransomware. https://www.trendmicro.com/vinfo/us/security/definition/ransomware, (Access date: 12 December, 2017)

Trochim, W.M., (2002). The Knowledge Base: An online Research Methods Textbook, trochim.human.cornell.edu/kb/index.htm, (Access date: August 23, 2011).

Tsai, S., Machado, P., (2002), E-learning, online learning, web-based learning, or distance learning: unveiling the ambiguity in current terminology, ACM Publication, http://elearnmag.acm.org/featured.cfm?aid=568597 (Access Date: 20 December, 2015).

Urdan, T.A., Weggen, C., (2000). Corporate e-Learning: Exploring a New Frontier, W R Hambrect and Co.

USA Patriot Act of 2001. H.R.03162, (2001). http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162, (Access Date: 11 December, 2009).

Usu, S., (2003). Advantages of Computer Based Educational Technologies for Adult Learners, The Turkish Online Journal of Educational Technology – TOJET volume 2 Issue 4, https://files.eric.ed.gov/fulltext/EJ1101937.pdf, (Access Date: 6 February, 2017).

Uto, N., Melo, S.P., (2009). “Vulnerabilidades em Aplicações Web e Mecanismos de

Proteção”. Minicursos SBSeg 2009. IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Campinas, São Paulo, Brazil.

Vaishnavi, V., Kuechler, W., (2005). Design research in information systems. January 20, 2004, last updated August 16, 2009. URL: http://desrist.org/design-research-in-information-systems.

Van Tiem, D.M., Moseley, J.L., Dessinger, J.C., (2012). Fundementals of Performance Improvement Optimising results through people, processes, and organisation. ISPI/Wiley.

Van Doorn, J.R., Van Doorn J.D., (2014). The quest for knowledge transfer efficacy: blended teaching, online and in-class, with consideration of learning typologies for non-traditional and traditional students. Frontiers in Psychology. 2014;5:324.doi:10.3389/fpsyg.2014.00324.https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029015/, (Access date: 12 September 2016).

Varshney, Y., (2017). Attacks on Digital Watermarks: Classification, Implications, Benchmarks. International Journal on Emerging Technologies (Special Issue NCETST-2017)

Veerappan, J., Pitchammal, G., (2012). Geometric attack resistant multilayer image watermarking scheme for providing high security.

Vesper, J. L., Kartoglu, Ü., Herrington, J. and Reeves, T. C., (2016). Incorporating risk assessment into the formative evaluation of an authentic e-learning program. British Journal of Educational Technology, Vol. 47, No. 6.

Volery, T., and Lord, D., (2000). Critical success factors in online education. The International Journal of Educational Management, 14(5), 216–223.

Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J. J., Su, J. K., (2001). Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. In IEEE Communications Magazine, vol. 39, no. 8.

Von Zezschwitz, E., Koslow, A., De Luca, A., Hussmann, H., (2013). Making Graphic-based Authentication Secure Against Smudge Attacks.In Proceedings of the 2013 International Conference on Intelligent User Interfaces (IUI ’13).ACM, New York, NY, USA,277–286. https://doi.org/10.1145/2449396.2449432.

Walls, J. G., Widmeyer, G. R., El Sawy, O. A., (1992). "Building an Information System Design Theory for Vigilant EIS." Information Systems Research, 3(1), 36-59.

Wang, F., Ge, B, Zhang, L., Chen, Y., Xin, Y., Li, X., (2013). A system framework of security management in enterprise systems. Syst. Res. Behav. Sci. 30(3):287-299.

Wang, P., Jiang, L., (2015). Task-role-based Access Control Model in Smart Health-care System. MATEC, Web of Conferences.

Wavemaker, (2017). Token Based Authentication, Learning Centre Documentation, https://www.wavemaker.com/learn/app-development/app-security/token-based-authentication/, (Access date: 15 January 2017).

Weatherley, M. (2014) Copyright Education and Awareness, a discussion paper, www.cubismlaw.com/wp-content/uploads/2015/06/mweatherlycopyright-education-awareness.pdf. (Access date: 1 April, 2016).

Weber, A., (2004). The Rhetoric of Positivism Versus Interpretivism: A Personal View. MIS Quarterly, 28 (1).

Weippl, E., (2005). Security in E-Learning (Advances in Information Security). Springer, New York.

Wiley, D., (2000). Connecting learning objects to instructional design theory: A definition, a metaphor, and a taxonomy. In D. A. Wiley (Ed.), The instructional use of learning objects: Online version. http://reusability.org/read/chapters/wiley.doc, (Access date: 26 April, 2011).

Wilkerson, J., (2009). Staff and student perceptions of plagiarism and cheating. International Journal of Teaching and Learning in Higher Education, 20(2), 98-105. Retrieved from http://www.isetl.org/ijtlhe/ ISSN 1812-9129.

Wilson, J., (2010). “Essentials of Business Research: A Guide to Doing Your Research Project” SAGE Publications.

Xu, W., Bhatkar, S., Sekar, R., (2006). Taint-Enhanced Policy Enforcement: A Practical Approach to Defeat aWide Range of Attacks. In 15th Usenix Security Symposium.

Yan, J. A. Blackwell, R. Anderson, and A. Grant, (2004). Password memorability and security: Empirical results. IEEE Security and Privacy.

Yin, R. K., (2003). Case study research: Design and methods, 3rd edition, London, SAGE Publications.

Yasin, M., Mazumdar, B., Sinanoglu, O., Rajendran, J., (2015). Removal Attacks on Logic Locking and Camouflaging Techniques. Journal of LATEX Class Files, Vol. 14, No. 8.

Yong, J., (2007). Security modelling for e-Learning, First IEEE International Symposium on Information Technologies and Applications in Education, ISITAE '07.

Zhang, G. and Parashar, M., (2003). Dynamic Context-Aware Access Control for Grid Applications.

Zhang, F., Kondoro, A. and Muftic, S., (2012). “Location-Based Authentication and Authorization Using Smart Phones,” in Proceedings of 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.

Zhou, Z., Wu, L., Hong, Z., (2013). Context-Aware Access Control Model for Cloud Computing. International Journal of Grid and Distribution Computing. 6(6), 1-12.

Zuev, V., (2012). E-Learning Security models, Management Information Systems, Vo. 7 No 2.