ANALYSIS OF SECURITY ISSUES IN CLOUD BASED E-LEARNING

Master’s (one year) thesis in Informatics (15 credits)
Gunasekar Kumar (S101261)
Anirudh Chelikani (S101405)

2011MAGI23
Title: Analysis of security issues in cloud based e-learning

Year: 2011

Author/s: Gunasekar Kumar (S101261)
               Anirudh Chelikani (S101405)

Supervisor: Jens Allwood

Abstract:

Cloud based E-Learning is one of the booming technologies in IT field which brings powerful e-learning products with the help of cloud power. Cloud technology has numerous advantages over the existing traditional E-Learning systems but at the same time, security is a major concern in cloud based e-learning. So security measures are unavoidable to prevent the loss of users’ valuable data from the security vulnerabilities. Cloud based e-learning products also need to satisfy the security needs of customers and overcome various security threats which attack valuable data stored in cloud servers.

So the study investigates various security issues involved in cloud based e-learning technology with an aim to suggest solutions in the form of security measures and security management standards. These will help to overcome the security threats in cloud based e-learning technology. To achieve our thesis aim, we used theoretical and empirical studies. Empirical study is made through the information gathered through various cloud based e-learning solution vendors websites. And the theoretical study is made through the text analysis on various research articles related to our subject areas. And finally the constant comparative method is used to compare the empirical findings with the facts discovered from our theoretical findings. These analysis and research studies are leads to find various security issues in cloud based e-learning technology.

Keywords: Security, Cloud based E-Learning technology, Security management standard, Security measures, Learning management system, Security threats
Acknowledgements

This master thesis presents the results of the study about “Analysis of security issues in cloud based e-learning”, which was conducted between April 2011 to August 2011 at the Department of Business and Informatics in University of Borås, Sweden.

First we would like to thank my tutor, Professor Jens Allwood, for his great support through the whole process, his guidance and encouraging attitude.

Additionally, we would also like to thank Professor Anders Hjalmarsson for ideas, articles and valuable assistance given during the thesis work.

Finally, we would also like to thank our friends and family members for their cooperation and understanding which helped us to complete this thesis.

Borås, August 2011

Gunasekar Kumar
Anirudh Chelikani
# Table of Contents

1 **INTRODUCTION** .................................................................................................................. 1

1.1 BACKGROUND ......................................................................................................................... 1

1.1.1 Relation to informatics ........................................................................................................... 2

1.2 STATEMENT OF PROBLEM ...................................................................................................... 2

1.3 PURPOSE OF THE STUDY ......................................................................................................... 2

1.4 RESEARCH QUESTIONS ............................................................................................................. 3

1.5 TARGET GROUP ......................................................................................................................... 3

1.6 DELIMITATIONS ......................................................................................................................... 4

1.7 EXPECTED OUTCOME ............................................................................................................... 4

1.8 THE AUTHORS OWN EXPERIENCE AND BACKGROUND ......................................................... 4

1.9 STRUCTURE OF THE THESIS .................................................................................................. 4

2 **RESEARCH DESIGN** ............................................................................................................... 7

2.1 RESEARCH PERSPECTIVE ........................................................................................................ 7

2.2 RESEARCH STRATEGY ............................................................................................................... 8

2.3 DATA COLLECTION PROCEDURES ........................................................................................... 9

2.4 DATA ANALYSIS PROCEDURES AND PROCESSES ............................................................. 9

2.5 STRATEGIES FOR VALIDATING FINDINGS ............................................................................ 10

2.6 RESULT PRESENTATION METHOD ........................................................................................... 10

3 **THEORETICAL STUDIES** ..................................................................................................... 11

3.1 KEY CONCEPT .......................................................................................................................... 11

3.1.1 Cloud Based E-Learning ..................................................................................................... 11

3.1.2 Security management ......................................................................................................... 11

3.1.3 Management Standards ....................................................................................................... 11

3.1.4 Information security ........................................................................................................... 11

3.1.5 Server Security .................................................................................................................... 11

3.1.6 Authentication ..................................................................................................................... 12

3.1.7 End User ............................................................................................................................... 12

3.2 SUBJECTS AREAS RELEVANT FOR THE RESEARCH ............................................................ 12

3.3 PREVIOUS RESEARCH ............................................................................................................ 14

3.4 RELEVANT LITERATURE SOURCE ......................................................................................... 14

3.5 KNOWLEDGE ON CLOUD BASED E-LEARNING ................................................................ 14

3.6 KNOWLEDGE ON CLOUD COMPUTING ............................................................................. 15

3.6.1 Cloud computing basics ..................................................................................................... 15

3.6.2 Cloud computing architecture ............................................................................................ 15

3.6.3 Types of cloud .................................................................................................................... 17

3.7 KNOWLEDGE ON E-LEARNING .............................................................................................. 18

3.7.1 E-Learning Basics .............................................................................................................. 18

3.7.2 E-Learning Environments .................................................................................................. 19

3.7.3 Future trends on e-learning ................................................................................................ 21

3.8 CLOUD BASED E-LEARNING ................................................................................................. 23

3.8.1 Mobile E-Learning .............................................................................................................. 24

3.8.2 Key Benefits of cloud based E-Learning ............................................................................ 24

3.8.3 Current limitations in Cloud based e-learning .................................................................. 25

3.9 SECURITY ISSUES IN CLOUD BASED E-LEARNING ............................................................... 26

3.10 SECURITY THREATS & CHALLENGES IN CLOUD BASED E-LEARNING ......................... 28

3.11 SECURITY MANAGEMENT STANDARDS IN CLOUD BASED E-LEARNING ....................... 32
4 EMPIRICAL SURVEY .................................................................................................................................. 45

4.1 PURPOSE ........................................................................................................................................ 45
4.2 SAMPLING ...................................................................................................................................... 45
4.3 QUESTIONNAIRE ............................................................................................................................. 45
4.3.1 Cloud E-Learning Company 1: “Moodlerooms Inc.” ................................................................. 46
4.3.2 Cloud E-Learning Company “Docebo Inc.” ............................................................................... 48
4.3.3 Cloud E-Learning Company “Blackboard Learn - ANGEL” ...................................................... 50

5 ANALYSIS AND RESULT .................................................................................................................. 53

6 DISCUSSION ..................................................................................................................................... 57

6.1 CONCLUSION ................................................................................................................................. 57
6.2 IMPLICATIONS FOR INFORMATICS ........................................................................................... 58
6.3 METHOD EVALUATION .................................................................................................................. 59
6.4 RESULT EVALUATION .................................................................................................................... 59
6.5 POSSIBILITIES TO GENERALIZE ............................................................................................... 60
6.6 IDEAS FOR CONTINUED RESEARCH ......................................................................................... 60
6.7 SPECULATIONS FOR THE FUTURE ............................................................................................... 61

7 BIBLIOGRAPHY ............................................................................................................................... 62

8 APPENDICES ..................................................................................................................................... 66

List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Structure of the Thesis</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Subject area relevancy for the research</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>Cloud computing architecture (Al-Jumeily et al., 2010)</td>
<td>16</td>
</tr>
<tr>
<td>4</td>
<td>Public cloud deployment model (Carlin et al., 2011)</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>Hybrid cloud deployment model (Carlin et al., 2011)</td>
<td>18</td>
</tr>
<tr>
<td>6</td>
<td>E-Learning system (Pocatilu et al., 2009)</td>
<td>19</td>
</tr>
<tr>
<td>7</td>
<td>Conceptual model of a PLE (Wilson et al., 2007)</td>
<td>21</td>
</tr>
<tr>
<td>8</td>
<td>Architecture of e-learning cloud (Laisheng et al., 2011)</td>
<td>23</td>
</tr>
<tr>
<td>9</td>
<td>Challenges for E-Learning cloud (Laisheng et al., 2011)</td>
<td>25</td>
</tr>
<tr>
<td>10</td>
<td>Results of IDC ranking security challenges (3Q2009, n=263) (Popovic et al., 2010)</td>
<td>27</td>
</tr>
<tr>
<td>11</td>
<td>SMS passcode login scenario (Ahmed et al., 2011)</td>
<td>40</td>
</tr>
<tr>
<td>12</td>
<td>Biometric system diagram (Ahmed et al., 2011)</td>
<td>41</td>
</tr>
<tr>
<td>13</td>
<td>Server security in cloud based E-Learning - Key results of Theoretical and Empirical study</td>
<td>54</td>
</tr>
<tr>
<td>14</td>
<td>E-Learners security in cloud based E-Learning - Key results of Theoretical and Empirical study</td>
<td>55</td>
</tr>
<tr>
<td>15</td>
<td>E-Learning materials security in cloud based E-Learning - Key results of Theoretical and Empirical study</td>
<td>56</td>
</tr>
</tbody>
</table>
## Abbreviations Used:

<table>
<thead>
<tr>
<th>Term</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBE</td>
<td>Cloud based E-Learning</td>
</tr>
<tr>
<td>SLA</td>
<td>Service level agreement</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a service</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a service</td>
</tr>
<tr>
<td>IaaS</td>
<td>Information as a service</td>
</tr>
<tr>
<td>LMS</td>
<td>Learning management system</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal digital assistant</td>
</tr>
<tr>
<td>ISO</td>
<td>International standard organization</td>
</tr>
<tr>
<td>SCORM</td>
<td>Sharable Content Object Reference Model</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information technology infrastructure library</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>DDoS Attack</td>
<td>Distributed Denial of service attack</td>
</tr>
<tr>
<td>CBET</td>
<td>Cloud based E-Learning technology</td>
</tr>
<tr>
<td>CCM</td>
<td>Constant comparative method</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

1.1 BACKGROUND

In this modern era, numerous technologies are being introduced day to day making the human life easier. Particularly web based technologies have a huge contribution in reducing the people's routine work. At the same time, many institutions and universities introduce some new courses to give knowledge about these technologies and make people techie to deal with them well. However, institutions are facing with lack of experienced teachers to teach those technical courses to their students. To override this problem, many institutions introduce online education service for those courses. Hence, E-Learning is one of the best and most important technologies which help them to create a good learning environment. Therefore, many countries including developing nations such as India are implementing the E-Learning software solutions to improve their educational standard. Although, they still have many problems regarding required facilities and infrastructure to implement the traditional E-Learning method to a wide range of educational institutes throughout the country. Thus, the cloud computing technology is a proper superseding the traditional E-Learning method to overcome this problem.

There are numerous advantages (see section 3.8.2) with substitutions of traditional E-Learning method by cloud computing technology. Cloud computing is portable and helps to make the e-learning solutions possible for mobile phones and other similar mobile devices such like as Tablet PCs, smart phones, PDAs. Cloud based e-learning solutions are very much helpful to reduce the cost in the traditional e-learning technology by its widespread cloud source. But still, there are some problems to be concerned when implementing cloud based E-Learning solutions to all educational institutes.

At the same time whatever technology is introduced in the market, people are concentrating more on the security features of those technologies irrespective of an electronic gadget or a web technology. People are very conscious on the security features of the technology when it comes to a web source, due to infinite vulnerabilities. Cloud based E-Learning technology is no way an exception from security vulnerabilities from the internet, when it deals with cloud power to enhance the features on an existing traditional e-learning technology. Since the E-Learning technology is not a new one to the technical field, it overcome already some problems to reach the current standard. So, it has many security standards to provide safety for the e-learning solutions and information of the end users on the server. Likewise cloud computing technology also has some security standards to maintain and provide security features for their end-users and investors from web vulnerabilities. But still the question is that whether cloud computing will fulfill and provide enhanced security to the e-learning technology, or create a security problem on the existing security features of traditional e-learning technology. In this thesis, those key security problems are identified along with the severity involved as a barrier and the possible solutions while implementing the cloud based E-Learning technology are explained.
1.1.1 Relation to informatics

A simple definition of informatics was suggested by Saul Gorn in 1983: “Informatics is computer science plus information science” (Gammack et al., 2006). In the book called “The book of informatics” by (Gammack et al., 2006) was mentioned that informatics is a field which covers the various academic fields related to information. As mentioned in that book, this thesis also deals with informatics where our main research is about the security measures and issues of cloud computing based e-learning systems and the information stored on those systems.

1.2 STATEMENT OF PROBLEM

In recent days many cloud computing companies emerge in market and offer the cloud power to many technical solutions to make their products more cost effective and enhance with the cloud power. The E-learning solution is one of those technologies where it implements the cloud power in its existing system to enhance the functionality providing to e-learners. E-learning is one of the widespread technologies, which helps to compensate the shortage of knowledgeable teachers in universities and many other institutes, so cloud computing makes its fortune by providing cloud power to the functionality of e-learning solutions. At the same time, security also needs to be addressed when cloud is implemented with e-learning solutions. So in this thesis, we study the key security issues in use of cloud computing in e-learning systems.

1.3 PURPOSE OF THE STUDY

Security is one of the people’s peak concerns on all grounds. People are more concerned of the security especially when using the gadgets or technologies that involve internet. Because the internet has many loopholes that can crash the application or hack the application to gain access to the users or company details by hackers worldwide. E-learning technology is now incorporated with many latest technologies to provide more provision and reduce the complexity from traditional e-learning methodology to their users. So in this thesis, we are mainly focused on the security issues in e-learning technology when it is implemented with cloud computing technology. Because cloud computing is one of the fast developing technology which offer numerous benefits and provisions to users who used to enhance their existing technology with cloud power. But still cloud computing has not achieved the fulfillment on security issues. So there is a question raised on how the cloud provides security in e-learning technology and to the e-learners. So our research throws light to identify the security issues with cloud based e-learning and the countermeasures took recently on those problems.
1.4 RESEARCH QUESTIONS

Main Question:
What can be the key security issues in use cloud computing for e-learning systems?

Sub-Questions:
1) What can be the Server security issues in cloud based e-learning?
2) What can be the E-learners security issues in cloud based e-learning?
3) What can be the E-learning materials security issues in cloud based e-learning?

1.5 TARGET GROUP

- ICT authorities from developing nations:
  Information and communications technology (ICT) authorities from the developing nations are our main target group, where the people are able to offer and build the good infrastructure facilities to all citizens of their nation, which helps to bring about an enhanced and successful implementation of cloud computing on e-learning systems.

- Investors of E-Learning & cloud computing solutions:
  The results of this thesis are hopeful to offer better solution to find out, improve and overcome the practical security problems to develop and implement cloud computing in e-learning technology. So, this is overall good news that benefits the investors and vendors involving in cloud based e-learning technology.

- Researchers on developing cloud based E-Learning:
  The outcome from this thesis helps to make improvement and find out the way to overcome the security problems in a better manner to develop an improved cloud based e-learning solutions. So, this thesis is hopefully having a research contribution which helps researchers to develop a better cloud based e-learning solutions.

- Universities & institutes using E-Learning technology:
  Many universities and high schools from various nations are sure to be benefitted from this thesis, in the way of getting better e-learning solutions with cloud support and also get solution for implement the better infrastructure for cloud based e-learning solutions with good security features.
1.6 DELIMITATIONS

Our thesis mainly focuses on security issues in cloud computing based E-learning solutions, so our thesis does not cover about other practical difficulties and problems in cloud based e-learning. Because of this, our thesis is only limited to security issues in cloud based e-learning and this is our delimitation too.

1.7 EXPECTED OUTCOME

The expected outcome of this thesis is to find out the key security issues and concerns taken on when implementing the cloud computing for e-learning systems. We also try to exploit the security concerns that e-learners and the end-users of cloud based e-learning solutions wants to get it from the cloud based e-learning solution vendors.

1.8 THE AUTHORS OWN EXPERIENCE AND BACKGROUND

We both acquired our bachelor’s subject with the major on computer science and information technology. There we studied the concepts that are related to system security and authentication methods used to protect the information. Especially the subjects like cryptography and system security teaches about the security techniques and methods used in various system to protect the data from hackers. Also our master’s subject deals with the informatics in which courses like System development philosophy, human information systems, and interaction design helps us to gain the knowledge about system design and its essential principles. Apart from the theoretical knowledge which we gain through our academic studies, we also have the knowledge about system security, e-learning, and the cloud computing from various sources and applications using in our daily life. Especially now-a-days cloud computing is involving in all the web applications like E-Mail, online communities like Facebook, online streaming videos like YouTube, etc. We also have knowledge about e-learning system from the Ping-Pong which we are using in our university, which helps us to communicate with other students and staff members of university, to know the class timings and upload/download the course materials like assignments and slides. So the knowledge and experiences that we gained through various sources are helpful to make this thesis to be a better one from our side.

1.9 STRUCTURE OF THE THESIS

The structure of our research area is fractioned into six chapters which are explicated by series of steps in a diagrammatical representation.

The first chapter begins with a short introduction to background of our work along with the future implications. In this chapter we also stated about the implication and relation
of our work to informatics. We parted the main research area into three sub questions which together lead to solve the principal problem of our study.

The second chapter comprise of our research strategy which is a plan of action that points the flow in the right direction and to check whether the process is carried out in a systematic procedure. In this chapter we further discuss about our research approach along with data collection procedures, data analysis procedures, result presentation methods and finally the strategies for to validate the findings.

The third chapter constitutes the theoretical base of our study which is the perspective to analyze and select the literature and establish an idea of how they relate to one another. So we had gone through the relevant literature sources and the previous research studies in order to frame out the foundation for our work. We identified the further issues and detailed it by choosing the crucial content from them. Then finally we accounted the summary of the theoretical findings followed by argumentation for the empirical study.

The fourth chapter structured on narrating the importance of the empirical study which is a research achieved only thorough self-observation or experimentation. This in turn used to making decisions in choosing the best option to get a job done. Our work is structured on comparative analysis. Along with that the data collection through different sources and methods like questionnaires are portrayed.

The fifth chapter is the key one which is the analysis of both theoretical and empirical results collected through sources in previous chapters. The results of the evaluation are assessed and interpreted, giving possible reasons for their occurrence.

The sixth chapter finally presents the method discussions and the result obtained accompanied by the final conclusion part. In this phase we also discussed about the further research scope of our study.

The reference section (Harvard Format) and the questionnaires for our comparative analysis study which are in the final appendix part are found after the chapters.

The whole thesis work is represented by a diagrammatical view which is shown below:
Figure 1: Structure of the Thesis
2 RESEARCH DESIGN

2.1 RESEARCH PERSPECTIVE

Research Approach:

The two main scientific perspectives are positivism and hermeneutics. Since my research aims at creating comprehension knowledge through interpretation, hermeneutics is the most relevant approach as it aims at interpreting and explaining meaningful concepts. (Verbeek, 2003)

For our research we choose hermeneutics as we are creating knowledge through the interpretation of concepts and text from various articles and web sources on cloud based e-learning and its security. Ricoeur builds on the thoughts and ideas of previous hermeneutists since he integrates hermeneutic theory, hermeneutic philosophy and critical hermeneutics. Ricoeur also adds a structural element since he means that it is impossible to reach meaning before a structural understanding. (Benediktsson, 1989)

According to Ricoeur perspective of hermeneutics without structural understanding it is not possible to gain meaning. In our research approach we adopted Ricoeur perspective as we are presenting our results to find out key security issues in CBE. We want to emphasize the role of cloud computing, traditional e-learning, security and other related issues while integrating cloud sources on traditional e-learning for attaining structural understanding of the cloud based e-learning and its security. And with the help of our empirical findings we demonstrate how the security issues are handled in real time by cloud based e-learning solution vendors. So by careful assessment of the situation from the results of theoretical and empirical studies are helps to bring the key security issues in cloud based e-learning. (Ricoeur, 2004)

Research Perspective:

There are three different distinctions for research studies that are widely used namely quantitative, qualitative and mixed study approaches. Quantitative studies which actually trust on quantitative data like numbers and figures, while Qualitative studies which actually trust on qualitative information like words, sentences and narratives whereas mixed approach is using both the statistical data in quantitative and the result orientation from qualitative view. So it is a mixture of both qualitative and the quantitative.

The following quote of verbal picture created by one textbook helps to distinguish between the Qualitative and Quantitative studies:

“Quality is the essential character or nature of something; quantity is the amount. Quality is that what; quantity the how much. Qualitative refers to the meaning, the definition or analogy or model or metaphor characterizing something, while quantitative assumes the meaning and refers to a measure of it’s… The difference lies in Steinbeck’s (1994) description of the Mexican sierra, a fish from the sea of Cortez. One can count the spines on the dorsal fin of a pickled sierra, 17 plus 15 plus 9. ‘But,’ says Steinbeck, ‘if the Sierra strikes hard on the line so that our hands are burned, if the fish sounds and nearly escapes and finally comes in over the rail, his colors pulsing and his tail beating the air, a whole new
relational externality has come into being. ‘Qualitative research would define the being of fishing, the ambience of a city, the mood of a citizen, or the unifying tradition of a group.’” (Blumberg et al., 2005)

Qualitative methods differ from quantitative methodology in various perspectives. Qualitative methods are viewed in a more theoretical way and result oriented when compared to quantitative method. The exploration aims are achieved through many numbers of ways and techniques. These aims are relevant for both quantitative and qualitative techniques, but even though this exploration of techniques relies highly intemperately on qualitative techniques.

**Qualitative Studies** is more suitable for our thesis problem, because we are going to compare the empirical results from three different worldwide cloud based e-learning solution vendor’s website with our theoretical findings. Later we are going to integrate them using constant comparative analysis to get the better output for finding the key security issues in cloud based e-learning. So for this comparative part and the data collection part of the thesis problem, qualitative studies are helpful for us.

### 2.2 RESEARCH STRATEGY

There are three different classifications of research strategy; they are descriptive, explanatory, and exploratory. Exploratory research is used for better understanding of problem and to test the quality of research findings or to develop a layout for further research investigations. Descriptive research is used as the statistical research which tries to explain the information and the features of the research findings. Explanatory research is used to describe the results by using exploratory and descriptive strategies to get further research findings.(Neuman, 2003)

In our research work we are going to use two types of research strategy:

**Exploratory:**

Exploratory study deals with the situations where the problem is not precisely defined. We have chosen exploratory study as our problem or situation includes an indefinite number of perspectives in the initial stages for to collect the knowledge about CBE. As we are navigating through finding different issues involved in implementing cloud sources on traditional e-learning we will be drive towards a specific and precise problem area which needs to find key security issues in CBE. (Cooper et al., 1998)

**Explanatory:**

We also have some inclination towards explanatory studies as they deal with relating different theories and concepts for enhancing the empirical study of a process. In our empirical study for finding the real time management by cloud based e-learning solution vendors against the security issues on their products, we are going to compare different perspectives of the same situation by three different companies to achieve a definite set of patterns that are used to make our theoretical findings strong. (Chisnall, 1981)
2.3 DATA COLLECTION PROCEDURES

In our thesis work, we followed various data collection procedures to generate the information which answers our research question. More specifically we used triangulation method as our primary data collection procedure to our study. Oates (2006) mentioned as “The use of more than one data generation method to corroborate findings and enhance their validity is called method triangulation”. Text analysis, observations, and questionnaires are the data collection procedures used in our thesis work. (Oates, 2006)

Text analysis is used as our primary data collection method, which helps to analyze research articles of various authors. It also combines the objective data from those articles to bring most appropriate result to our research question.

Prevalent observations in our thesis helped to find the current happenings in cloud based e-learning technology and its relative fields. These observations are collected through various online technical magazines like zdnet, cnet, etc. So these help us in the acquirement of knowledge about latest security trends and issues in cloud based e-learning.

Questionnaires are the primary data collection procedures followed in empirical study, which help to bring the answers to our theoretical findings. Questionnaires are prepared on the basis of support to our theoretical findings. Apart from that it also frames to collect some additional information from the CBE solution vendors on our research questions. More information about the questionnaires in our research study is explained in detail in section 4.2 and 4.3.

Article search for Theoretical Study:

We used various online sources like Google scholar, IEEE explorer, BADA, LIBRIS to collect materials for our thesis work. Apart from those online sources, we also used our University library to collect the articles for our theoretical study. We used some list of keywords to filter the articles in online sources, which brings the appropriate related articles for our research. Some of those keywords are cloud based e-learning, security in cloud technology, security in e-learning, security in cloud based e-learning. Apart from these keywords we use many manual and automatic filters in those search engines to find the exact articles that we expecting for our thesis work. Additionally we also used to search for the research articles that are mentioned in references of our previous findings. This strategy helped us to gather more knowledge on our research work to seek findings on research questions.

2.4 DATA ANALYSIS PROCEDURES AND PROCESSES

Strauss & Corbin (1990) mentions the importance of the processes and also stress to provide special attention to processes happens in research study. Data analysis procedure and processes are most important aspect in writing research articles. These procedures help to give the quality and reliable outcome on the thesis results. So we followed various procedures to analyze the data which we used in our thesis report. At first, we grouped our theory findings into different subject areas, to recognize and then used the data exactly on required
section of thesis. And after that, interpretation is used on articles to extract the objective data for our report work. Cross check our theory findings with various other articles also helped to ensure the reliable outcome for our research questions. The empirical findings are used to analyze our theoretical findings with the facts discovered from various cloud based e-learning vendor’s websites on security issues in it. (Strauss et al., 1990)

As we mentioned already in section 2.1, we had chosen the qualitative perspective approach to our thesis study. So, Constant comparative method is used as analysis in our thesis report, which helped to compare our theoretical and empirical findings together to bring the key security issues in cloud based e-learning. Because Boeije (2002) mentions that “The constant comparative method (CCM) together with theoretical sampling constitutes the core of qualitative analysis in the grounded theory approach and in other types of qualitative research”. Empirical results which are gathered through the various cloud based e-learning vendors websites are crosschecked with our theoretical findings through this constant comparative method. So the CCM helps to bring strong base for our theoretical findings by results of empirical study. (Boeije, 2002)

2.5 STRATEGIES FOR VALIDATING FINDINGS

We believe that validating our thesis findings is more crucial to verify our results and interrupting them with various strategies. We have used four different evaluation criteria for validating our thesis results. Michael Quinn Patton (2002) mentions that the four evaluation research criteria are to ensure the aim of thesis study. These criteria’s bring the valuable contents with quality results with more trustworthiness in overall findings of thesis study. The four different evaluation criteria’s are Quality, Validity, Reliability, and Generalizability.

There is a reason behind why we choose these four different evaluation criteria’s to validate our thesis findings. All these four different evaluation criteria have some unique thing which helps to verify our thesis findings and brings the accurate results. Quality has been used to ensure the richness and significance of our thesis results. Validity has been used to validate our theoretical findings through the help of comparative analysis with the empirical findings. Reliability has been used to ensure the trustworthiness of our sources which used as a base for our theoretical and empirical study. And finally, generalizability has been used to generalize our thesis findings to other groups which likely related to our subject area. Section 6.4 is clearly explained the way we chosen to ensure the quality, validity, reliability, and generalizability of our thesis findings. (Patton, 2002)

2.6 RESULT PRESENTATION METHOD

The results of the thesis are presented in figures so as to facilitate easiness in understanding the data and our analysis. Apart from diagrams, we also use texts to express our thesis results.
3 THEORETICAL STUDIES

3.1 KEY CONCEPT

3.1.1 Cloud Based E-Learning

Cloud based e-learning is the technology which is migration of traditional e-learning techniques on cloud computing technology to enhance the e-learning environment with numerous provisions to improve the learning experience of e-learners. (Pocatilu et al., 2009)

3.1.2 Security management

Security management is the field which relates to asset management, physical security and human resource safety functions. The main aim of the security management is to protect the overall organisation from various kinds of security attacks. Security management varies for each and every field based on the core line which deals with the respective field. The main objective of the security management that deals with internet and network is to protect and ensure the user safety, information security, server security from various attacks, and protect the total system from various Virus attacks like Spam, WORM, Trojans, and Trapdoors. (Dhillon et al., 2000)

3.1.3 Management Standards

Management standards are used to ensure the quality of management and the services offered to their customers. Management standards are varied for each and every field based on the core line which deals with the respective field. Management standards are offered to the organisation for the quality of their services by many international organisations such as International Standard Organisation (ISO), World-Wide-Web Consortium (W3C), American national standard institute (ANSI). (Svensson, 2001)

3.1.4 Information security

The security measures taken by the organisation or the individual user to protect the information on their system or products from the hackers are called information security. Information security methods are varied based upon the area of field where they are used like governments, military, corporate companies, hospitals, financial companies, and educational institutes. There are so many laws enacted by governments to make information security stronger against information stealing by hackers and unauthorised persons. (Dhillon et al., 2000)

3.1.5 Server Security

Servers are the storage units which store all the information for the web sites and web applications. The security of servers is important because servers deal with data of large number of individuals and organisations. So server security and server management is a big
deal and numerous security measures are taken to save the data in server from hackers and natural disasters. Usually many websites like Google, yahoo have more number of backup servers to give safety to their user’s data from server crash or overloading or other kind of security issues of server. (Scarfone et al., 2008)

3.1.6 Authentication

Authentication is a method followed to authenticate the valid user to use the product. This is a security measure which helps to avoid the intruders to hack the product or to access the products functionality to make malfunction. There are numerous authentication methods and techniques which are followed in the world of information technology. Based on the value of data on system, the Authentication methods vary. (Needham et al., 1978)

3.1.7 End User

User who uses the product and enjoys the full functionality of product’s outcome is called an end user. End users are the customers of the companies for their products. Based on the expectation and demand of the end user, the companies modify their product till the user gets satisfied with products of the company. The product which satisfies the end user is called as a successful product in the market. (iwebtool, 2011)

3.2 SUBJECTS AREAS RELEVANT FOR THE RESEARCH

In this section, we discuss subject areas which contribute in acquiring the results of our research questions. We narrowed down the key concepts in the subject areas as:

1) Knowledge on Cloud based E-Learning
2) Security threats in Cloud based E-Learning
3) Security measures taken in Cloud based E-Learning
4) Security Management Standards using in Cloud based E-Learning

The diagrammatical representation below explains how the subject areas are relevant for our research question and how they help to answers it.
Figure 2: Subject area relevancy for the research
3.3 PREVIOUS RESEARCH

While performing literature review for the study we found many articles on cloud based e-learning, security issues in cloud computing as well as in e-learning. Although we couldn’t find exact previous research work on our selected research question “security issues in cloud based e-learning”, we found numerous articles on individual areas and subjects. We searched mostly through online sources like Google scholar, IEEE explorer, and Google search engine. They were helpful to gain knowledge on security threats, security measures, and security standards involved in cloud computing as well as e-learning technology. Based on this knowledge, we developed a framework for our thesis.

3.4 RELEVANT LITERATURE SOURCE

We reviewed the literature and found many articles which dealt with the subject areas of our study. These research articles explained about the cloud based E-Learning and security issues in cloud computing. The following articles provided a strong theoretical framework for our thesis.

- The research article on “Cloud computing security issues and challenges” (Popovic et al., 2010), which gives information on security problems in cloud computing technology and the security measures taken to overcome these security problems.
- The research article on “Cloud computing: a new business paradigm for E-Learning” (Laisheng et al., 2011) which describes the cloud based e-learning, benefits of cloud based e-learning, and the practical difficulties on implementation of that technology.
- The research article on “Privacy and security in E-Learning” (El-Khatib et al., 2003), also gives some key points on security issues in E-Learning technology and the security measures taken to overcome those security problems.
- The research article on “Strategy approach for eLearning 2.0 deployment in Universities” (Casquero et al., 2010) throws light on planning and development of the E-learning 2.0 and the e-learning technologies.

3.5 KNOWLEDGE ON CLOUD BASED E-LEARNING

Cloud based E-Learning is a technology that took shape by enhancing the existing E-learning technologies and methodologies with the help of cloud computing technology. Some important key concerns are to be taken into account when the institutions use the cloud for their E-Learning systems. So before proceed to a discussion on cloud based E-Learning, it is essential to keep light on the concepts of E-Learning and cloud computing and how both of the technologies are integrated in order to accomplish this concept.
3.6 KNOWLEDGE ON CLOUD COMPUTING

3.6.1 Cloud computing basics

Cloud computing is one of the popular buzzword used all over the IT world. Cloud computing word is actually derived from the way the internet is often signified in network diagrams (Pocatilu et al., 2010). Cloud computing defines the feature given by computation resources through a computer network. In a traditional way of computing, the user’s computer holds all the important software and data to perform all computing operations on those files. But in cloud computing, user’s computer almost don’t need to have anything for make computing on files except minimal operating system with browser and excellent internet connectivity (like broadband) to access files and applications from online sources. Many companies like IBM, Microsoft, HP, Dell, VMware, XenSource, etc., are investing on virtualization platforms. They are not only investing to bring easier access of their applications to their customers, but also bringing their power on next generation cloud technology. (Popovic et al., 2010)

There is no exact definition for cloud computing till now. However the work of Ian Foster et al in the paper “Cloud Computing and Grid Computing 360-Degree Compared” provided a general definition of cloud computing: “A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet.” (Foster et al., 2008)

Another definition given by (Vaquero et al., January 2009): “Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure Provider by means of customized SLAs.”

3.6.2 Cloud computing architecture

Cloud computing architecture mainly consists of three layers called IAAS, PAAS, and SAAS. These three layers are helpful to serve the variety of services to their customers from cloud vendors.

- **IAAS:** Infrastructure as a service is a provision that offers from the cloud vendors to their clients through the sources like storage, hardware, severs, 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 virtualization, there are two different kinds of virtualization:
1. **Full virtualization**: when one system or installed software from one machine can run another entire virtual system by its own emulation in it.

2. **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.

- **SAAS**: Software as a service, the name itself implies that the software’s like word processors are offered to their customers through the cloud for almost free or low cost. So the cloud users need not waste huge amount of money on get 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.

- **PAAS**: Platform as a service which 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)

![Cloud computing architecture](image)

**Figure 3**: Cloud computing architecture (Al-Jumeily et al., 2010)

Cloud computing clients may use one or more services of cloud computing based on their business needs. There are plenty of ways to access cloud computing through various forms of clients. Hardware devices like PDAs, mobile phones, regular PCs, notebooks, and software applications like regular web browser are such examples to access cloud computing from various clients. Cloud computing becomes most popular on all business sectors nowadays because it helps a lot to reduce the cost of use of software applications and hardware usage. Cloud computing helps to reduce the processor and memory usage through its online backup and applications. The clients may get online memory space on demand from cloud vendors with minimal cost while the real physical memory depends on their work needs. Many online applications like spreadsheet and software applications are helpful to clients to use the applications at minimal cost or free on demand and it helps to avoid purchase the license to use real time software applications. In some cases, some software applications like spreadsheet have offline support also from cloud vendors, in this case the process in offline mode get synchronized once it gets refreshed in an online mode. There are plenty of multi-national companies now offering best cloud computing solutions, like as
Google, Amazon, IBM, Yahoo, and Microsoft. Google’s API is best example for the cloud computing applications; Google offers plenty of software applications with the help of cloud such as YouTube, Google apps, Picasa. The main advantage of cloud computing is that one need not worry about client machine, because all our data is stored safely in online cloud. But still cloud computing have few disadvantages, such as subscription fee for the access cloud sources may become costlier for long term use, and it is always recommended for clients to use more than one client vendors to avoid data loss in case of any problems affected to cloud vendors like bankruptcy. (Pocatilu et al., 2010)

3.6.3 Types of cloud

Cloud computing have four different clouds which vary on their modes of deployment of computing:

- **Public cloud:** Public cloud is conventional way of cloud computing, where the third party vendors are provide the IAAS, SAAS, and PAAS. In this methodology, the user can have the access to these services on an ad-hoc basis through the cloud.

  ![Public cloud deployment model](image)

  **Figure 4:** Public cloud deployment model (Carlin et al., 2011)

- **Hybrid cloud:** Hybrid/enterprise cloud has both In-house and third party providers. In these kinds of clouds, some portion is private where it can be accessed only internal and the remaining portion is public which can be accessed externally.
**3.7 KNOWLEDGE ON E-LEARNING**

### 3.7.1 E-Learning Basics

With the advancement of computer technologies day by day, work becomes simplified with the help of preprogrammed software applications. E-Learning is one of the most famous technologies discovered to make the traditional way of education learning easier with the help of software applications and virtual learning environment. The word “E” means the electronic way of learning in the E-Learning. There are various names that are used to express the term E-Learning in a technology world such as Computer based training (CBT), Internet based training (IBT), and Web based training (WBT). These terms express the way of E-Learning teaches the lesson to the e-learner. E-learning comes through a network enabled computer and transfers the knowledge from the internet sources to end users machine. Usually the E-Learning works with the help of software applications and usually the information is transferred with the help of internet, audio/video files, satellite TV, media disks. These materials are having the contents like text, image, animation, audio/video to deliver the learning materials to E-Learning users. Many universities and institutions are implementing the e-learning for their distance education programmes and also used it to enhance the ability of other educational degree programmes. Cloud computing, mobile learning, communication technology, etc. are of help to bring the E-Learning to next level of IT world. (Welsh et al., 2003).
3.7.2 E-Learning Environments

E-Learning environment is nothing but the environment which offers through E-Learning applications to the students to get the access the materials and tools relating their studies. Virtual learning environment and personal learning environment are two important E-learning environments which offer the wide range of facilities to students through e-learning applications for their studies.

3.7.2.1 Virtual Learning environment

Virtual learning environment (VLE) is simply another term used to represent the E-Learning systems, where the students are able to get face to face class room environment through computer applications with the help of web sources. VLE is enhanced application from blended learning approach. The main objective of VLE is to provide the e-learning facility to large number of student communities to provide the virtual class room environment. There are many terms which are very similar to Virtual learning environment. They are learning management system (LMS), Content management system (CMS), Learning content management system (LCMS), Managed learning environment (MLE), Learning support system (LSS), Online learning centre (OLC), Open courseware (OCW), Learning platform (LP). Virtual learning environment basically works with the help of internet and provides the learning materials and tools to e-learning users for uploading files, chatting, and web conferencing. It also gives information regarding student group management systems,
questionnaires, peer assessment, wikis, blogs, 3D virtual learning classrooms, online feeds like RSS. Many universities and institutions are using VLE to improve the intractable learning environment and break the interaction barrier on learning environment. The foreword of the book “Virtually There” by Yorkshire and Humber Grid for Learning Foundation (YHGfL) (Wikipedia, 2011) is quoted here:

“Learning is breaking out of the narrow boxes that it was trapped in during the 20th century; teachers' professionalism, reflection and ingenuity are leading learning to places that genuinely excite this new generation of connected young school students — and their teachers too. VLEs are helping to make sure that their learning is not confined to a particular building, or restricted to any single location or moment.” (Eaves et al., 2007)

The main advantage of VLE, it is capable of storing many courses at a time, so it creates better environment for the instructor as well as the student when they are moving from one course to another. Apart from this facility, VLE provides some other provisions:

1) Notice board for up to date course information  
2) Students can take their courses at any time and from any convenient place to them.  
3) Students are allowed with special needs and restrictions to use this kind of e-learning systems.  
4) It provides the geographical wide spread education.  
5) It offers the education facility through internet which helps students as it is cost effective and flexible.  
6) Small universities which don’t have many elective courses are able to provide wide range of elective courses for their students in their institutions.  
7) It enables more intractability among the students and lecturers.  

(Kumar et al., 1998)

3.7.2.2 Personal Learning Environment

Personal learning environment (PLE) is a single user E-Learning system which helps the E-Learners to manage and modify their own learning. PLE is mainly used to integrate the WEB 2.0 technologies like Wikis, blogs, online feeds, online social communities with the independent E-Learners. PLE offers wide range of supporting features to their users, some of the important provision are:

1) Users can fix their learning goals on their own in the e-learning system.  
2) Users can manage the E-Learning systems both the learning materials and processes in the system.  
3) Users can communicate with other users in the same e-learning system in the learning process.  

(Van Harmelen, 2006)

Stephen Downes (Downes, 2006) describes the PLE as “one node in a web of content, connected to other nodes and content creation services used by other students. It becomes, not an institutional or corporate application, but a personal learning center, where the content is reused and remixed according to the student's own needs and interests. It becomes, indeed, not a single application, but a collection of interoperating applications—an environment rather than a system”.

20
3.7.3 Future trends on e-learning

Since the E-Learning technology is a not a new technology, it comes with the combination of latest technologies to enhances its provisions to e-learners. There are many new forms of e-learning methodologies to provide educational facilities to e-learners with variety of new provisions to enhance the functionality and e-learning environment. In those e-learning 2.0 plays a vital role on bring the e-learning to next level of internet based learning. After the evolution of web 2.0, e-learning is adopted the web 2.0 with the combination of iPLE (Institutional Learning environment) to bring the new technology called e-learning 2.0. E-learning 2.0 is nothing but to make e-learning environment to be more efficient than before with lot of new provisions to e-learners using online sources like blogs, forums, wikis, online communities, streaming videos, cloud sources, video/audio conferencing etc. There are so many sub forms created for e-learning after the evolution of e-learning 2.0 namely mobile learning, cloud based e-learning, blended learning. (Casquero et al., 2010)
3.7.3.1 Blended learning

Blended E-Learning is a concept which was used initially in UK in 1997. There are so many definitions given by many researchers for Blended learning and mentioned in the journal:

1) “A learning programme where more than one delivery mode is used.”
2) “Blended learning is the learning that is facilitated by the effective combination of different modes of delivery, models of teaching, and founded on transparent communication amongst all parties involved in a course.”
3) “Blended learning combines face-to-face instruction with computer mediated instruction. It is the combining of these two different learning environments, taking the specific benefits that each environment provide, greater access to improved learning experiences and doing so in cost-effective manner.”

(Patil et al., 2010)

Blended learning is the integration of traditional face to face class learning with e-learning techniques and applications. In this way, there are many e-learning tools used to create a class room environment through computer applications. Blended learning approach involves various kinds of teaching methodologies, learning strategies, education materials, learning skill development programs to improve the learning for e-learners. Blended learning helps to integrate the synchronous and asynchronous learning approach, so that every process taken in learning is pre-planned effectively to give high standard of education to students. In blended learning, students have the full rights and freedom to take the decisions and can make changes they want on their course. So blended learning is also called student centred approach. Even though students have more advantage in this approach, teachers also have more freedom and they can structure the student lessons, improve the speed of course period to facilitate quick learning ability to students. Moreover, teachers are able to give the course material which they like to teach to students through this blended learning approach (Hu et al., 2010). There are many ways to improve the student interaction through blended learning, they are:

1) Group discussion
2) Seminars
3) Workshop
4) Debate
5) Brainstorming
6) Collaborative learning
7) Cooperative learning
8) Interview
9) Field visit

Many kinds of technical materials are used to improve the quality of education through blended learning, they are:

1) CD/DVD
2) E-Mail
3) Chat
4) Video conferencing
5) YouTube
6) Online presentations
3.8 CLOUD BASED E-LEARNING

Cloud based e-learning is the sub division of cloud computing on educational field for e-learning systems. It is the future for e-learning technology and its infrastructure. Cloud based e-learning has all the provisions like hardware and software resources to enhance the traditional e-learning infrastructure. Once the educational materials for e-learning systems are virtualized in cloud servers these materials are available for use to students and other educational businesses in the form of rent base from cloud vendors. Cloud based e-learning architecture is explained in the following figure:

![Figure 8: Architecture of e-learning cloud (Laisheng et al., 2011)](image)

Cloud based e-learning architecture is mainly divided into five layers called hardware resource layer, software resource layer, resource management layer, server layer and business application layer.

1) **Hardware resource layer:** This is bottom most layer in the cloud service middleware where it handles the essential computing things like physical memory and CPU for the total system. This layer is most important for the total infrastructure of the system. With the help of virtualization, physical servers, network and storage are grouped and called it as upper software platform. To offer the uninterruptable power to the cloud middleware services for the cloud based e-learning systems, physical host pool is expanded dynamically and memory is scalable at any time to add additional memory.

2) **Software resource layer:** This layer is created with the help of operating systems and middleware. With the help of middleware technology, many software solutions combine to offer the grouped interface for the software developers. So, software developers can create many applications for e-learning system and able to embed those in cloud, which helps the cloud users to compute those applications through cloud.
3) **Resource management layer:** This layer plays an important role on get loose coupling of software and hardware resources. With the help of virtualization and scheduling idea of cloud computing, it brings the uninterrupted on-demand software distribution for different hardware resources.

4) **Service layer:** Service layer is divided into three levels namely IAAS, PAAS, and SAAS. These service layers help to cloud customers to use the various forms of cloud resources for their products like software resource, hardware resource, and infrastructure resource.

5) **Business application layer:** Business application layer differs from all other layers in cloud based e-learning architecture, because this layer acts as important business logic of e-learning, and frames the expansion of group of components for e-learning. Business application layer mainly consists of content creation, content delivery, education platform, teaching evaluation and education management.

   (Laisheng et al., 2011)

### 3.8.1 Mobile E-Learning

Mobile technologies are one of the fastest going 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 android, Microsoft, apple, 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. So e-learners can able to use the e-learning sources from either PC or Mobile phones/Tablet PCs. (Rao et al., 2010)

### 3.8.2 Key Benefits of cloud based E-Learning

There are numerous advantages when the e-learning is implemented with the cloud computing technology, they are:

1) **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)
2) **Improved performance**: Since 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)

3) **Instant software updates**: Since the cloud based application for e-learning runs with the cloud power, the software’s are automatically updated in cloud source. So always e-learners get updates instantly. (ibid)

4) **Improved document format compatibility**: Since some file formats and fonts do not open properly in some PCs/mobile phones, the cloud powered e-learning applications do not have to worry about those kinds of problems. As the cloud based e-learning applications open the file from cloud. (ibid)

5) **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., 2009)

6) **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)

### 3.8.3 Current limitations in Cloud based e-learning

While the cloud based e-learning is having numerous advantages, still there are some disadvantages in cloud computing to e-learning technology. Those limitations in cloud based e-learning technology are discussed in this section:

- **Charge**: When cloud computing is used for e-learning systems, charges are very crucial in the overall system - how the cloud vendors charge the schools and individuals. The solution to this problem is not to follow the market oriented charge mechanism. That means, they need to combine the school fees and individual fees

![Figure 9: Challenges for E-Learning cloud (Laisheng et al., 2011)](image)
instead of charging the school for using general resources and charges the individual for using special resources.

- **Bandwidth:** Since the cloud based e-learning fully depends on the internet sources, bandwidth plays a vital role to deploy the data in internet servers. One way to solve the problem is to develop fibre optical network to provide the better bandwidth for using the cloud resources for e-learning educational environment.

- **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.

- **User idea:** Infrastructure of cloud computing, IT service delivery, and usage patterns used in cloud based e-learning undermines the traditional way of using computer technology. So it will lead to affect the e-learning user’s ideology and their acceptance on further development on cloud based e-learning. To avoid this problem, there is need to build the good case models for cloud based e-learning and need to promote their applications widely to reach more e-learners.

- **Educational forms and methods:** The main challenge for e-learning technology is the replacement of traditional educational forms and methods. But e-learning is not entirely removing the importance of teachers in its technology; instead it gives more freedom for teachers to build the environment which they like to provide for the students. So to overcome these issues, teachers need to involve themselves in cloud based e-learning applications.

- **Education management rules:** Traditional learning environment varies from e-learning environment. In this case if cloud is used for e-learning systems there may be a chance for new problems on learning environment through cloud based e-learning. So to overcome this problem, suitable management rules are to be maintained for cloud based e-learning. Teaching content management, course management, examination management, performance management, student management, teacher workload management, etc. are to be structured.

- **Resource development:** In any technology, the stakeholders need to be involved in its development to bring the best outcome from its usage. When it comes to cloud based e-learning technology, the teachers, and other educational experts should be involved in its resource development to bring the best set of scientific, interesting, and artistic learning resources.

  (Laisheng et al., 2011)

### 3.9 SECURITY ISSUES IN CLOUD BASED E-LEARNING

Security issues are more important in this kind of technologies as it ensures the reliability of technology in users’ mind to handle it. Since the cloud based e-learning fundamentally depends the web based sources for its operational functionality, there are numerous threats waiting to attack the e-learners and the cloud based e-learning technology through the internet. Even though cloud provides plenty of advantages to e-learners, the cloud security is still in doubt for its security issues/challenges in a digital world. International data corporation (IDC) which conducted a survey with the 263 IT executives to estimate their
mind-set on use of cloud services for their IT companies, they ranked the security as first for greatest challenges/issues of cloud computing. (Popovic et al., 2010)

![Figure 10: Results of IDC ranking security challenges (3Q2009, n=263) (Popovic et al., 2010)](image)

IDC survey on cloud security challenges is one of the good examples to show the IT peoples and other stack holders concerns on security issues when implements the cloud services for their products. Nowadays, There are so many major IT companies like GOOGLE, MICROSOFT, AMAZON are become cloud vendors and provide their cloud services to various kind of users around IT world for various purposes. All these companies are already famous for their trustworthy applications and services to IT world, but still peoples are have doubts about cloud safety from those companies. So those companies are following many security standards and measures to ensure the security in their cloud products and services. In the same time, E-Learning solution vendors also have security standards and measures to overcome problems on e-learning applications and its security in e-learning materials and e-learners. Since cloud computing alone is not our track, we discuss the both cloud computing and e-learning technology’s security issues and measures separately to find out the key security issues and measure for cloud based e-learning.

In these days huge investments are applied in the field of e-learning by several countries as there is a fact that the development of a country depends on the investment on the infrastructure in the field of education. From the past decade with the trend in the IT Industry and growing speed of the internet sources, there is a lot of scope to provide the education for the large number of people with ease. One can learn and gain the knowledge with less effort and with minimal requirements. Factors like expenditure, cost of the hardware in the case of e-learning was very effective and simple and one can easily acquire the required knowledge from many sources in that field. Along with the growing demand and popularity for the e-learning there are several security threats which grow along with the technology. There are several issues related to privacy are to be analyzed and also there is a need to implement several security functions and tools for the case of e-learning in order to solve all the issues related to the security. These functions are not only some specific software variances but also related to the hardware and also in some cases the combination of
both of them like biometric etc. E-Learning is implemented when both information and communication systems have to work together and by using other kinds of electrically enabled technologies. E-learning includes several types of learning such as web based learning, computer based learning, virtual classroom etc. There are several logically located areas for e-learning at a similar time. Along with the other implications like technology, speed, reliability, flexibility of the e-learning systems security and privacy must also be considered as an integral part for those systems. (Ahmed et al., 2011)

So in this section of this paper, we discuss the cloud computing and e-learning technology security issues and also find out the measures and standards to overcome key security threats in cloud based e-learning.

3.10 SECURITY THREATS & CHALLENGES IN CLOUD BASED E-LEARNING

Since Cloud based e-learning is combination of cloud computing and e-learning technologies, in this section, we first discuss about key security concerns and threats involved in cloud computing technology and later about e-learning technology.

A) Cloud computing security threats:

Since the cloud computing offers numerous services provides to the various applications and technologies, some of key security concerns in cloud computing are mainly deals with server security and the information security stores in cloud sources from various technology and applications. Those key challenges and threats in cloud computing are as follows:

1) Basic Security concerns:

Some of the basic security concerns when using cloud sources to enhance the functionality of technology are listed here:

- Physical security is lost with the cloud model control, because companies don’t have the knowledge or control of running resources when they share the computing resources with third party companies.
- In most cases, a company violates the law when they use cloud services. And also there is a chance of data seizure by foreign nations.
- Most of cloud vendor’s services are not compatible with other cloud vendors. So it may be becomes a problem when the company tries to move their sources from one cloud vendor to another.
- When e-learning solution providers use the cloud source, a question arises on who should control the authentication procedures. Usually customers only have those encryption/decryption keys.
- Cloud providers need to ensure the data integrity by authorized transactions such as transfer, storage, and retrieval of data. For this problem, cloud providers need to follow same standards to ensure this problem on integrity issues.
Customers need to process against cloud vendors if customer’s privacy rights are violated. Cloud providers should provide clear answers on how the customer’s personal information is used or leaked to third parties. Cloud vendors should provide the updates regularly to their customers to ensure up to date security.

(Popovic et al., 2010)

2) Availability:
Availability of important applications and information on cloud servers for uninterrupted service to customers are the main concern cloud computing. A Denial-of-service attack (DoS Attack) or Distributed-Denial-of-service attack (DDoS Attack) are the popular online attacks which affect the availability of online servers, and thereby makes the servers and the data stored in it are unavailable for the users. Due to such attacks there were many incidents of cloud outage such as Gmail (one-day outage in mid-October 2008)(Chow et al., 2009), Amazon S3 (over seven-hour downtime on July 20, 2008)(Chow et al., 2009), FlexiScale (18-hour outage on October 31, 2008)(Chow et al., 2009), Google’s blogger outage (over 48 hours downtime on May 12, 2011) (Bott, 2011), and Gmail reset problem ( accidently resetting Gmail accounts on Feb 27, 2011) (Hollister, 2011).

3) Data Lock-in:

Nowadays cloud providers offer numerous tools, applications, standard data formats to their customers. But these services face problems when a customer tries to move to some other cloud provider, because mostly cloud providers are not compatible with one another. So customers are forced to stick with same cloud provider and cannot migrate to another cloud operator’s services. This problem creates a dependency issue on those cloud operators to get continued service. (JAMIL et al., 2011)

4) Insecure of Incomplete data deletion:

In most operating systems, data is not deleted completely even after the data erased from their physical machine. Customers are not able to know, whether their data is fully wiped out from all the virtual machines once after the delete command is applied. This problem leads to unsecured data on cloud. And also there may be a risk of this stolen data being used by unauthorized persons or hackers from the cloud. (ibid)

5) Increased Authentication demands:

Cloud providers offers various advantages to their customers, one of them is to provide software and its application access through online. So client machine need not be installed with any software applications to access for its functionality. Users need not bother about software piracy as these are run by centralised monitoring servers through cloud. But cloud providers should be careful to provide authentication to their customers for access by authorized persons. If cloud operators fail to provide these authentication procedures, it may lead to increase the threat of phishing or other vulnerabilities through unauthorised access of those applications on cloud. (Chow et al., 2009)
6) Browser security:

Cloud computing actually depends on remote servers for each and every computational tasks to be done. Client machine is only used with I/O devices to access any software applications. In this case, browser in client machine is the gateway to access the cloud servers. So browser security is crucial on total cloud security, because if the gateway is attacked by malware, then total cloud security becomes a problem. Modern web browsers here come up with the AJAX techniques like JavaScript, XML HTTP Request, Plugins which can operate I/O devices. Security policies and authentication certificates must be needed to ensure browser security. XML signature and XML encryption also help to ensure the browser security issues. (Jensen et al., 2009)

B) E-Learning security Threats:

E-Learning security threats are nothing but the security problems which questions the safety of the users who work with e-learning environment. This section deals with the key security threats involved in the e-learning systems apart from cloud based security threats for cloud based e-learning.

1) Basic E-Learning security concerns:

Basic security concern of E-Learning technology usually arise when we use it enhance the functionality of traditional learning environment. They are listed here:

- **User authorization and authentication:**
  
The user authorization is very essential and important when it comes to e-learning. In general the e-learners are from distant places, so provided with a user id and a password. With the use of these one can login into the e-learning server and can access the features.

  The learner or the student can access the billing account according to the levels. Based on the billing method he may or may not be allowed to the next level of the learning provision.

- **Entry points:**
  
  Entry points are the number of terminals or passive ways where a possibility of security breach may occur in the case of E-learning. As there are number of clients in distant locations for each e-learning server there is lot of entry points for each of them and possibility of a security threat is more. In order to get rid of this threat the designers have to reduce the number of entry points. But it cannot be implemented as there are number of clients in different physical and geographical locations at the same time.

- **Dynamic nature:**
  
  One of the major concerns with the e-learning is more processes are available in the dynamic sessions where a process can join and end the session without the notice of the others. This is vulnerable for much security infracts where they can easily attack the server and the client locations. To get rid of this type of happenings one should have to maintain strict sessions and several security credentials have to be maintained at both the sites i.e., client and server.
• **Protection against manipulation:**
  Protection against manipulation is one of the key tasks to be implemented in an e-learning environment. It is specifically implemented in the case of students where manipulation is more possible. It can be prevented from the other users by using certain techniques like digital signatures, firewalls etc. similarly several other measures have to be taken in order to avoid manipulation from the registered users. Thus e-learning environment gets enhanced by following and using the security measures carefully which will create a smooth structure of data flow along the network.

• **Non-Repudiation:**
  In the step of information security, cases of data loss or infection with virus, Trojan horse and other malicious treats are common. The system must be provided with the capability that the data is not modified by these attacks.
  (Ahmed et al., 2011)

2) **Social aspects of security:**

   Online e-learning environment is different from tradition learning environment. The main change is submission of assignments by students to teachers. In the traditional learning environment, students submit their assignments in hard copy format to their teachers directly in class rooms. Whereas in online e-learning environment, students need to upload their soft copy of assignment. So, this kind of methods in e-learning technology brings the threats and vulnerabilities from internet to e-learning systems. To overcome these problems, basic security requirements such as the integrity, confidentiality and availability are to be observed. Those security concerns are explained in detail here:

• **Confidentiality:** Confidentiality is an important aspect in security concerns, where the data or information sent through online is to be kept as secret and not to be disclosed to unauthorised 3rd party. Under e-learning perspective, students like to get the assurance that their submitted soft copies of assignments through online are kept secret and only revealed to their teachers on e-learning environment.

• **Integrity:** Information or data is not accidentally or maliciously deleted or changed, and it should be kept accurate as in original form. Students feel assured if integrity standards are maintained. This can happen only when their assignments submitted to teachers are kept safe in original format without any further edition by others.

• **Availability:** The reliable information should be present to access and modify it by authorised persons. Information present in e-learning servers must be present for students and teachers or other authorized persons on timely manner for their work. Students need assurance for uninterrupted reliable e-learning system to submit their assignments.

   There are two main types of availability attacks which create problem on e-learning systems for the availability issues, they are (Ahmed et al., 2011):

   i. **Blocking attack:** In this attack generally the e-learning content will be attacked by the external user and he obtains the permission to access the e-learning material. In this case one has to monitor the attackers IP address and block that address in order to get rid of this problem.

   ii. **Flooding attack:** Flooding attack is the one where huge amount of requests to a specific service or large amount of data in the form of small messages are sent blocking the entire service or the session. This may also cause the loss of availability for more time due to processing delays. The counter measures for
these types of attacks are to efficiently validate the incoming request or the message.

(Raitman et al., 2005)

3.11 SECURITY MANAGEMENT STANDARDS IN CLOUD BASED E-LEARNING

There are so many management standards used throughout the world for every technology or product to ensure its security. Since the cloud based e-learning is combination of two different technologies, we need to consider both technologies and its security standards to know the overall management standards to ensure the security of cloud based e-learning.

1) Security management standards using in cloud computing sector:

A) Information technology infrastructure library (ITIL):

ITIL is a set of rules that define an integrated and process-based operation to deal with the information technology services. It is utilized and implemented in almost all IT sectors including cloud computing. ITIL offers a systematic and professional access to the IT management and their services and helps to get good information security measures on all levels like strategic, tactical and operational levels. ITIL operations consist of many iterative processes like control, plan, implement, evaluate, and maintain. The main problem on ITIL is that only practitioners can be certified as “ITIL-compliant”, so organisations and other management systems are not able to get certified as “ITIL-compliant”. IT sectors which implement and use ITIL guidelines get many benefits, some of them are:

- Cost efficiency.
- IT services are improved by ITIL’s best policies and guidelines.
- Customers are more satisfied through a better service delivery with professional approach.
- Production becomes better and improved through ITIL’s guidelines.
- ITIL helps to differentiate the administrative and technical tasks separately, so it brings more effective ways to assign the appropriate resources.
- ITIL helps to bring effective third party services delivery through its speciation or ISO 20000 as the standard on service procurements.
- ITIL helps to use the experiences in efficient way.

The ITIL-process Security management explains the overall planning for management organisation to fit the information security. This process is basically depends on the practice code used for the information security management which is now called as ISO/IEC 27002.

ITIL helps to crack the information security down into:

- Policies: This is the main goal of an organization which tries to achieve.
- Processes: These happen when the policy goals are achieved.
o Procedures: These procedures are to identify the persons and also to mention what and when he/she needs to perform the goals.

o Work instructions: These Instructions are helps to perform the specific tasks for perform the goal.

The main aim of security management is to control and ensure enough information security. The ultimate aim of information security is to save information/data from the security attacks. Usually these goals are explicated in terms of assuring the confidentiality, integrity and availability, which along with associated attributes or aims such as authenticity, accountability, non-reputation and reliability.

B) International organization for standardization (ISO) 27001/27002:

ISO/IEC 27001 basically determines the compulsory demands for an information security management system (ISMS). These standards also uses and certification standard for ISO/IEC 27002 to show the desirable information security controls among the ISMS.

Basically the ITIL, ISO/IEC 20000, and ISO/IEC 27001/27002 models help the IT sectors to respond and answer some fundamental questions like as:

o “How do I ensure that the current security levels are appropriate for your needs?”

o “How do I apply a security baseline throughout your operation?”

o “How do I ensure that my services are secure?”

C) Open Virtualization Format (OVF):

OVF helps to provide the efficient, flexible, distribute secure software. It provides the mobility of virtual machines and the platform independence to customer’s vendor. Customers are able to use OVF formatted virtual machine on their existing virtualization techniques. OVF offers numerous benefits to their customers to enjoy the enhanced virtualization with more flexible, portability, signing, versioning, verification, platform independence and licensing terms. OVF also help for customers like:

- user experience is improved with the help of streamlined installations
- customers get platform independence on using virtualization
- customers are easily able to create the difficult pre-configured multi-tiered services
- mobile virtual machines help to deliver the enterprise software with more efficiently
- extensibility helps customers to adopt their technology easily in virtualization and also helps by providing platform based enhancements

(Popovic et al., 2010)
2) Security management standards using in E-Learning technology sector:

To develop an online e-learning solution there are number of 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 standardization and compatibility. There is also a factor to check whether different e-learning systems are compatible with one another or not. There are several working groups which are seeking to develop the standards for the e-learning sources. Those groups suggest the principles and standards concerned mostly on the sharable components and other resources. Principles involved in them also suggest the privacy and the security issues involved in the e-learning solutions. Some of the groups which work in the proposal and in development of these standards are (El-Khatib et al., 2003):

- IEEE LTSC: IEEE Learning Technology Standards Committee
- IMS GLC: IMS Global Learning Consortium
- AICC: Aviation Industry Computer-Based Training Committee
- ARIADNE: Alliance of Remote Instructional Authoring and Distribution Networks for Europe and
- ADL-SCORM: Advanced Distributed Learning-Shareable Content Object Reference Model

In the Sections below we review the standards involved along with the privacy and security concerns involved in them.

A) IEEE P1484:

IEEE P1484 is the model which was proposed by IEEE LTSC. 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 like 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 about 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 if the learner information gets accredited in server it will become de-identified, partitioned and compartmentalized which will cover most of the privacy and security factors related to the user.

B) IMS LIP:

The IMS global learning consortium (IMS GLC) is an organization intended to develop open specifications for distributed learning. 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 & packaging specification, question and test specification,
Simple sequencing specification, and learner’s Information Package specification. 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.

It employs different ways to capture Learners’ information which includes his 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. By employing the learners’ Information server the Learning system can be efficiently utilized by the user. For maintaining privacy and security for the learners, information for providing better support to the learner, enable certain mechanisms in the IMS LIP specification. 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. 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.

i) **The privacy and data protection meta-structure:** If we consider a learner information tree structure, each tree node and leaf is associated with the set of privacy description which consists of privacy levels, access rights and data integrity. The granularity of information can be defined as the set of data which cannot be further breakdown the independent privacy data.

ii) **A "security key" data structure:** In general, password, public key and digital signatures can be considered as the security keys. Structure of the security key, the password and security codes are used for communication. Based on the structure we can allow the public key encryption, data authenticity, and password –based access control on learner information.

C) **Other E-learning Standards:**

For distance learning systems there are standards and some industrial organizations working on specifications. They are Aviation Industry CBT [Computer-Based Training] committee (AICC), the Alliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE), and the Advanced Distributed Learning-Sharable Content Object Reference Model (ADLSCORM). But most of them are providing very little reference to security and privacy but are concentrating more on content management, meta-data specification.

**For example:**

- The AICC focuses on practicality and provides recommendations on e-learning platforms, peripherals, digital audio, and other implementation aspects.
- The 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)
3.12 SECURITY MEASURES IN CLOUD BASED E-LEARNING

From the previous research on cloud computing threats, we know the severity of problems involved in cloud based e-learning technology and for its vendors, as well as the e-learners. Cloud based e-learning technology also uses some sort of management standards and other security measures to overcome the security vulnerabilities and threats. Since cloud based e-learning is combination of two different technologies, we need to consider the both technologies on security measures and methods used to overcome security threats.

A) Security measures taken in cloud computing:

There are several security measures taken to overcome the security threats involved in cloud computing technology by cloud vendors as well as international committee for cloud computing organisation. These security measures answer how to overcome the security problems we discussed earlier. Those security measures are:

1) Software-as-a-Service (SaaS) security:

SaaS is a cloud service model in which most of the security practices and oversight will reside. Before adopting the service model by the corporations or end users they need to know the vendor policies on data security before using their services so that if they can block the unintended access of the data. The Gartner lists even security risks which one should discuss with a cloud-computing vendor before buying cloud-computing services.

i) Privileged user access: The users should gather information from the various management people who are accessing the data. They need to get useful information and oversight of all the privileged administrators, and the control over their access.

ii) Regulatory compliance: one should make sure that the vendor should be ready to undergo external audits and/or Security certifications.

iii) Data location: While using the cloud computing services we are not sure of where our data resides. It can store in various countries so that the cloud computing service vendors should be willing to accept the rules and regulations of the jurisdictions, and should undergo the contract with the local privacy requirements on behalf of their customers.

iv) Data segregation: The data should be able to encrypt at all the stages, and the encryption algorithms should be tested by experienced professionals.

v) Recovery: The cloud should provide the facility to recover the data and the infrastructure if the cloud has undergone some unintended attacks which can render the system complete destruction. So the vendor should provide facility to completely recover the data even after the destruction of the data.

vi) Investigative support: If an unintended attack or illegal activity occurred on a cloud computing source one cannot easily investigate where it’s from. The users can login from multiple locations and from variety of host and data centers. The vendors should be able to provide privileges for the specific investigation along with the evidence that such activities are supported by the vendors. This investigation of the attacks can be done systematically.

vii) Long-term viability: In a business context it’s quite common for the service provider to be acquired by a big company. Even then the customer or the user
should be able to access the data and acquire all his data. In such a situation, the SaaS providers are expected to incorporate such security management practices to develop new ones for cloud computing environments.

2) **Security management (People):**
   For organizations which provide technology based services it’s obvious to have a security team. To make it possible for the employees or team members to reach their potential there should be a charter formulated clearly depicting the roles of the members of the security team. Lack of such proper plan that details the roles of the members of the security team renders the organization to be a failure.

3) **Security governance:**
   A committee on security issues can be constituted in the organization. The main goal of this committee is to provide guidance and assistance regarding the security issues that align with the organizations strategies. The committee must clearly define the roles and responsibilities for the organization in providing information security functions.

4) **Risk management:**
   Risk management involves a variety of tasks such as identification of technical assets and data and its direct indications to the business processes and applications, data stores, etc. The owners of the organizations have the authority and obligations along with accountability for the information assets that includes custodian’s confidentiality, integrity, availability, and privacy controls.

5) **Risk assessment:**
   Risk management is an important business process that keeps the organization informed while moving forward in taking a new step or a decision. The risk management helps the organization to decide on whether it could go for a new decision or not. The main challenge for risk management is to give equal priorities for the users or customers interest along with the security. Security assessments like threat modeling are recommended to be implemented with the applications and infrastructure.

6) **Security awareness:**
   Creating security awareness is also one of the important actions that need to be done. Lack of proper security awareness can make them to reveal or expose vital data of the organization which in turn can cause the organization vulnerable to threats. Social engineering attacks, lowering reporting of and slower responses to potential security incidents can cost huge loss to the organization which is a result of poor security awareness.

7) **Education and training:**
   This involves in providing proper training about the fundamental security issues and risk management skills for the security team and their internal partners. This involves in identifying the set of skills of the security team members and to provide them proper training and mentorship that can be as broad base of fundamental security, inclusive of data privacy, and risk management knowledge.
8) **Policies and standards:**

For developing policies or standards for the cloud computing systems it’s always a good idea to take into consideration the already available templates and resources. The first and foremost important task of the security team is to consider data security along with the business requirements. These policies should strictly provide with proper documentation which supports the policies and standards. For maintaining relevancy these standards and policies should be revised from time to time with considering significant changes that occur in business or IT environment.

9) **Third party risk management:**

Lack of third party risk management can be of a huge loss for the organizations reputation, revenue losses due to the negligence on the part of the third party vendors.

10) **Vulnerability assessment:**

This is useful in classifying network assets to create enough significance and space for vulnerability-mitigation programs such as patching and system upgrading.

11) **Security image testing:**

Virtualization-based cloud computing is helpful in creating “Test image” VM secure builds and to clone multiple copies. Gold image VMs provides the system to be up to date that reduces the exposure due to patching offline. Offline VMs can be patched off network which helps in providing better usage of resources with less cost and less production threatening way to test the security changes on the system.

12) **Data governance:**

This framework mainly involves the roles by various stakeholders in data access and actions to be performed and the methods to be employed.

13) **Data security:**

Security to the data is demanded for the cloud based technologies that are present now in the market. The Organizations can provide encryption of certain types of data, which make it possible for the specified users to access the data. This also can provide compliance with the payment card Industry Data Security Standard (PCI DSS).

14) **Application security:**

Application security is all about the security features and requirements of application program and its interface. Application security is also used to review the security test results of application. Security team and development team work together to bring the efficient application security processes, guidelines for secure application coding, training, scripts using for testing and tools. Even though product development engineering teams concentrate on security design of application layer and its infrastructure layer, security team must supply the security requirements for the product development engineers to bring the best security measures and to implement their ideas.

15) **Virtual machine security:**

Cloud environment is usually grouped many physical servers into virtual servers to operate the virtual machines. In this cloud environment, not only the cloud
vendors and their data security teams are secure the virtual machines to implement the important security controls for the data center. Those data security teams also give the guidelines to their customers to prepare their virtual machines and its security for cloud environment.

16) Identity Access Management (IAM):
IAM is one of the most important operations for any organization where the basic expectation from the SaaS customers on “Principle of least privilege” is allowed for their information stored in cloud servers.

17) Change management:
Change management is the work taken by security teams under cloud vendors, in that they make some set of rules and guidelines for security management standards and the other small modifications in security measures. These guidelines are to give the self-service capability to the system to adopt those changes, which help to reduce the security team’s time and resources to prioritize for those modifications on security measures and production.

18) Physical security:
Cloud computing does not allow their customers to have the access for the physical assets, so the security model should be reevaluated. Even though cloud computing customers valuable data is not stored in their own physical memory, but still their data is stored in somewhere on physical location of cloud vendor’s. A huge financial budget needed to build high level security for physical data centers. That is the main reason behind the avoidance of companies to build their own data centers and for immigration to cloud services. So cloud vendors are needed to take many security measures for their physical data centers like:

1) 24*7*365(366) onsite security
2) Biometric security installation for access physical assets
3) Security cameras need to watch all the activities on physical properties throughout their service
4) Physical servers and other assets of cloud vendors should be maintained with right temperature, air flow, and humidity.

19) Disaster recovery:
When considering SAAS environment, the customers expect that the systems to respond and provide services 24/7/365 without any hassles. Using virtualization software virtual server can be copied, backed up, and can be easily relocated like a simple file.

Benefits are:

- No downtime are required to reallocate the computing resources in case of any natural or other kind of disaster affects the cloud servers.
- Able to provide and deliver the service level agreements (SLA) with high quality service.

20) Data privacy:
There is a need for constituting a committee for supporting in the decision making process that is related to data privacy. Another way of doing is to employ or hire a privacy expert, consultant in that area. This can create confidence for the customers that organization can meet data privacy needs. (Popovic et al., 2010)
B) Security measures taken on e-learning:

There are number of security measures taken up to overcome the security threats and vulnerabilities in cloud based e-learning by various vendors and organizations involved using this technology. Apart from all these security measures, e-learning technology already have some mechanisms to handle the vulnerabilities over internet and other incoming threats for its technology to protect e-learning materials and e-learners from those attacks. Those security mechanisms are discussed here:

1) **SMS security mechanism:**

This process is used for the authentication of a legitimate user into the e-learning environment. The procedure is same like in the case of “team viewer” where a user at first logged into the e-learning server with the help of a user name and a password which is provided during the registration period. After entering into the environment the user will get a pass code for that specific session in the form of an SMS (Short Message service) to his mobile phone which is registered in the server and thus security is maintained. As the logging phase of the user is specified from session to session with the different pass code it is mainly used to stop the provisions or illegal entry into the e-learning server from the outsiders or illegitimate users.

![Figure 11: SMS passcode login scenario (Ahmed et al., 2011)](image)

2) **Biometric Mechanisms:**

It is the mechanism in which the security is maintained. It gives allowance to the legitimate user by using one or more of their own physical or behavioral attributes. During the registration phase, one collects the physical traits of a user like finger prints, iris recognition or behavioral traits like voice recognition etc. and they will be stored in the database. During the login of the user the attributes of them will be compared to the one which is stored in the database by the use of some biometric scanning devices like finger print mouse etc. If both of them are same the content of e-learning is provided to the user. In this process it involves the physical presence of the user which is very keen, reliable and secure.
3) **Security Token:**

   It is a common way of issuing authentication by many universities for their students where they provide a hardware security token. It is sometimes called as a cryptographic token and its acts like a key to gain access into the e-learning system. It is further provided with a password mechanism by showing the identity electronically and entering the password one can gain access to the system.

4) **ACL mechanism:**

   ACL or Access Control List mechanism is the process to gain access to the server or the specific resources. In this the user can access their mechanism by using customization factor. The ACL factor will be attached or in built in the file. For example we want to add the user “Shane” to gain access to the system then we have to specify user “Shane” into the ACL file so that he can gain access to the system. We can also give several other functions to the user like “read, write, delete”: This option will give access to the user Shane to read, modify or to delete the specific file. These are all host based mechanisms and all the permissions are confirmed under the control of the service provider.

5) **Digital Signatures:**

   Digital signatures are used to authenticate the identity of a sender. In this it is easy to find out whether the original content in the message has been modified or not. It consists of mainly three contents. At first an electronic signature has been generated from the sender while sending the message to the receiver from an insecure network. Along with the message and the signature, the sender will submit a certificate sort of thing which is produced from a hash algorithm and private key from the sender’s computer. The main advantages with these digital signatures are to provide non-repudiation. Even though sender claims that he did not sign a message and kept his private key secret, we can claim that by using some non-repudiation algorithms which can produce a time stamp with that we can authorize and claim that the message has arrived from the sender. We can also check whether the data has been modified by the intended user.
6) **Security from passive attacks:**

In all the above methods we discussed about the active attacks from the outers. In case of passive attack one will not make any effect on source or the destination systems but the cipher text or in some case the plain text will be modified by the attacker. By using modern ciphering methods we can avoid these types of attacks. By using certain cryptographic methods like private key cryptography, public key cryptography and hash functions we can avoid passive attacks.

(Ahmed et al., 2011)

### 3.13 SUMMARY OF THE THEORETICAL FINDINGS

From the above mentioned theoretical discussion, we came to know one thing that is the Newton’s third law of motion:

“For every action, there is an equal and opposite reaction.”

For all the threats and vulnerabilities over the cloud based e-learning technology, cloud vendors and researchers are ready to give a counter attack. These threats and counter measures are going to be explained here. We like to separate the results of our theoretical findings into sub divisions, which are likely to answer our research questions of the thesis.

**RQ1. Server security in cloud based e-learning:**

Servers play a vital role in cloud based e-learning technology. So the server security is more essential than anything. From our theoretical findings the key security threats in cloud based e-learning servers are analyzed and listed here:

1) Availability
2) Increased authentication demands

In order to overcome these security threats on servers, there are numerous security measures and security management standards which are being followed by cloud based e-learning solution vendors. They are:

1) Disaster recovery
2) Physical security
3) OVF security management standard

**RQ2. E-learners security in cloud based e-learning:**

E-Learners are the main stakeholder of cloud based e-learning technology, so security concerns about e-learners are crucial. We also observed some of the key security threats faced by e-learners in this technology are:

1) Browser security
2) Social aspects of security
3) User authorization and authentication
Further, some counter measures and security management standards are in use by cloud based e-learning solution vendors. They are:

1) SMS security mechanism, biometric mechanism, ACL mechanism
2) Security token
3) Digital signatures
4) Security from passive attacks
5) XML signature and encryption methods
6) Security awareness
7) IEEE P1484 & IMS LIP Security management standards

**RQ3. E-learning materials security in cloud based e-learning:**

E-Learning materials are nothing but the information/data which is used to teach the e-learners, and the data stored in server to run the cloud based e-learning solutions. These materials play a vital role on teaching e-learners through online by e-learning solutions. So if someone or some attack malfunctions or deletes these materials from cloud based e-learning solutions through server attacks or by any virus codes, it makes a huge security problem. So, the security concerns on e-learning materials used in cloud based e-learning are very important for the technology. We gather some key security threats over e-learning materials which are used in cloud based e-learning technology. They are:

1) Data lock-in
2) Insecure of incomplete data deletion

To overcome these security threats on e-learning materials in cloud based e-learning technology, some counter measures and security management standards are used by cloud based e-learning solution vendors. They are:

1) Data privacy
2) SaaS security
3) Security management standards:
   a) ITIL
   b) ISMS
   c) ISO/IEC 27001
   d) AICC
   e) ARIADNE

**3.14 Arguments for an Empirical Study**

The practical experience always serves better than theoretical knowledge. Though we gathered lot of information on security issues of cloud based e-learning through our theoretical findings from various research articles, it’s worth to cross check our theoretical findings and its results in real life with the help of the empirical study. We like to subject the empirical study on the following aspects:

- Whether the cloud based solution vendors are following security management standards and other security measures over security threats in cloud based e-learning technology or not?
• Apart from our theoretical results, are there any other practical security threats attacking the cloud based e-learning technology?
• What are all the other security measures and security management standards in use to avoid security threats over cloud based e-learning technology?
• E-learning solution vendors feel cloud is secure and give more provision for e-learning solutions than traditional e-learning technology.
• What are the future plans on cloud based e-learning technology to make it totally secured.
4 EMPIRICAL SURVEY

4.1 PURPOSE

The purpose of this empirical survey is to find the practical influence of our theoretical findings in real life by cloud based e-learning solution vendors. Empirical survey is one of the most powerful way to analyze the problem and also best procedural way to collect data for the study. In this study, Theoretical findings help to find the numerous security threats and security measures in cloud based e-learning. Empirical survey helps to validate those theoretical findings on our study. So, final outcome from this empirical survey and the theoretical findings brings the strong result for our study. The main concept of our study is to analyze the security issues involved in the cloud based e-learning. For that, this empirical survey helps to bring the reality facet of security vulnerabilities and security measures taken in the cloud e-learning field. These results are cross checked and analyzed with our theoretical findings to answer the research question of our study.

4.2 SAMPLING

Sampling is the efficient way to conduct the empirical survey for the research study, because conduct survey to all range of stake holders is such a difficult task in a shorter time. So, sampling helps to get the reliable result by select the few stakeholders for our research. Oates (2006) mentioned as “A sampling frame is some kind of list or collection of the whole population of people (or events or documents) that could be included in your survey, from which you will choose a sample”. In this empirical survey, we choose three of the popular cloud based e-learning solution vendors as our sampling for this research. Since our complete thesis depends on the security provided by cloud e-learning software vendors, we plan to ask questions these companies to know the practical security issues in cloud based e-learning technology. (Oates, 2006)

4.3 QUESTIONNAIRE

This questionnaire is chosen to collect the practical security issues in cloud based e-learning technology. Here, we like to gather the information on security threats and the security measures taken by cloud e-learning software solution vendors to protect their servers, users and other valuable data. Nowadays almost all the top software providers provide their company’s information in their websites, either in a form of frequently asked questions or in the form of white paper about their company or in the form of overview of their product. So we plan to get the information for our questions by text analysis through the websites of cloud e-learning software vendors.
4.3.1 Cloud E-Learning Company 1: “Moodlerooms Inc.”

Question 1: Company’s profile

Moodlerooms, Inc. is a USA based cloud E-learning solution vendor. This company is founded by Tom Murdock, Sheila Gatling and Gina Russell Stevens in the year 2005. Moodlerooms is using an open source Moodle at its core for provide an open, accessible, and flexible learning management platform. Moodlerooms is a one of the largest worldwide Moodle partners with more than 700 clients in 2009; some of the important clients are Major corporations like Cisco, Schools like Frederick County Public schools and Universities like Louisiana state university and California State University. To develop there E-Learning products and services, they developed strategic partnerships and plugins with other e-learning technology leaders like Cisco, Dell, iParadigms and Datatel. (Moodlerooms, About Moodlerooms, 2011)

Question 2: Products & services offering to customers

Moodlerooms offering various e-learning services and products to their customers with the help of Open source Moodle at their core. Some of the E-Learning services they offer are Hosting service, support service, implementation, training, course conversion, and customisation. Apart from these services, Power and Joule are the two important e-learning solutions offering by Moodlerooms to their customers. (Moodlerooms, LMS Solutions, 2011)

Question 3: Are you own your server for your products and services? If not, you have full access for your outsourced servers?

No, Moodlerooms are outsourced their server needs for their products and services to Dell cloud hosting company. Because Moodlerooms believes that outsourcing servers are allow providing the uninterrupted server source and unlimited space for their products and services which offers to their customers. So Moodlerooms are using Dell cloud services as their cloud hosting for all of their E-Learning products and services, which is located in Plano, TX.

Even though Moodlerooms used Dell cloud hosting service as their outsourced server, but still that company has full access to monitor and work on their outsourced servers from Dell cloud hosting service. (Moodlerooms, Hosting - Moodlerooms on the Cloud, 2011)

Question 4: Security management standards taken against security threats on their products

All the Moodlerooms products and services are having SCORM and IMS complaint for interoperability of content. So this security management standards are ensures the Moodlerooms E-Learning products are having good level of security feature which offers to their customers. (Moodlerooms, Create an Secure, Collaborative Training Environment, 2011)
Question 5: Security measures taken by company against server security threats

Moodlerooms, Inc. is using the Dell cloud hosting for their server needs, so all the server security measures are taken by Dell cloud hosting company to protect their servers from various vulnerabilities on servers. The server security measures taken by Dell cloud hosting company are listed below (Moodlerooms, Hosting - Moodlerooms on the Cloud, 2011):

1) Dell cloud hosting servers are secured with various physical security measures, such like as 24x7 armed security and CCTV surveillance, Multi-level security card readers with battery backup, and Biometric scanning.
2) Dell is used Load balancers and firewalls in their datacentres, which helps to filters the vulnerable information and adjust the data load to their servers.
3) Dell cloud hosting data centre is certified by SAS 70 type II.
4) Regular vulnerability tests within the virtual environment is regularly conducted by Dell and Moodlerooms on their cloud environment to run all known attacks, which helps to discover and find remedy for any threats.
5) To provide the highest level of data security to the clients, Dell and Moodlerooms are expertise with HIPAA, FERPA, GLBA, CA SB 1386, Sarbanes Oxley and Basel 2.

Question 6: Security measures taken by company against the threats in cloud e-learning users

Moodlerooms provides the high level security to their users, who use their products and services. Security measures which taken by Moodlerooms for their users are listed below (Moodlerooms, Hosting - Moodlerooms on the Cloud, 2011):

1) **Password protection:** Moodlerooms used MD5 hash security mechanism to keep secure their user’s login information. Apart from that, Moodlerooms enforced the users to create effective user passwords to meet the specified criteria, which is achieved through enabling strong password policies.
2) **Authentication:** Moodlerooms provides wide range of security support to their users from external sources with the help of more than 15 authentication methods, which includes LDAP, IMAP, CAS, Shibboleth, POP3 and RADIUS.
3) **Virus scanning:** Moodlerooms uses Clam Anti-virus, which helps to protect the servers from various viruses from other computers as well as avoid downloading the viruses into the client’s computers from the servers.
4) **Roles-Based Access:** The user-role system provided by joule is very sophisticated. The access control for the content and delegating the administration through it is very advanced.
   - **Role** – From this one identifies the users status or their authorization level
   - **Capability** – It is to describe the particular feature associated with a role
   - **Permission** – The essential to be assigned for potentiality in a specific role
   - **Context** – The one surrounds a unit of language and helps to influence its interpretation
Question 7: Security measures taken by company to protect the e-learning materials and other information in their system

Information security is taken as a top most priority in the design of open source Moodle from Moodlerooms organization. So it ensures that all the data stored in the server is safe and secure.

It is designed in such that the security is under the control and customization of the administrator of the base. The information access is controlled through roles-based access, several authenticated logons and keys for enrollment. If the company is looking for a higher level security, SSL certificates i.e., uses a third party, a certificate authority (CA) are available for the intent.

Advantages for Information Security:
- The granular assignment of user roles and permissions is possible.
- The illegible access is protected by enrollment Keys used.
- SSL certificates which work on SSL protocol are available which are used for secure transactions between web servers and browsers
- Major government and health care organizations using this Secure Cloud hosting architecture

Valuable Features for Information Security:
- MD5 hashed password storage which is effective in checking the data integrity.
- Wide range of authentication methods(15 and more)
- 4-layer granular role system
- Enrollment keys
- Unique IDs
- Multiple administrators

(Moodlerooms, *Create an Secure, Collaborative Training Environment*, 2011)

4.3.2 Cloud E-Learning Company “Docebo Inc.”

Question 1: Company’s profile

Docebo is the Italian based Cloud E-Learning company which creates the open source E-Learning platform called DoceboLMS. DoceboLMS is not have any licence fees and used throughout the world by many organisations. Docebo have worldwide branches in many nations, such as Hong Kong for Asian branch, Dubai for Middle East branch, Herndon for USA branch, and finally headquarters in Milan for Europe branch. Docebo also have wide range of worldwide customers, in that some of prestigious customers are: Accenture, SHAPE financial Corp, RINA, AON, COOP, MEDIASET, Volks Bank, RIELLO, SARA, iPER. DoceboLMS is training more than 200,000 users on its cloud edition; this is one of the biggest achievements by Docebo Company. (docebo, *Docebo E-Learning solutions*, 2011)
Question 2: Products & services offering to customers

Docebo is offering various products and services to their users through its cloud e-learning technology. Those Cloud E-Learning products are Docebo LMS, Multimedia Contents, and Mobile Learning. (docebo, E-Learning solutions overview, 2011)

Question 3: Are you own your server for your products and services? If not, you have full access for your outsourced servers?

Docebo owns the datacenter which hosting the 24x7 Server storage and operational functionality for their cloud E-Learning products and services. So, Docebo have all the functional rights to operate and makes change on those servers at any time, and no need to get any 3rd party authentication for operate those servers. (docebo, DoceboLMS E-Learning Platform, 2011)

Question 4: Security management standards taken against security threats on their products

Docebo is certified by SCORM and ISO 9001. These security management standards certifications are helps to express the companies capable on fight against security threats over their e-learning products and services. (docebo, Why choose DoceboLMS?, 2011)

Question 5: Security measures taken by company against server security threats

DoceboLMS is an open source platform which allows customers to install the DoceboLMS on their own servers or any cloud hosting servers. Apart from that Docebo also provides high quality server support for their services and products. Docebo follows many security measures to protect their cloud hosting servers from various threats over there servers. They are:

1) HTTPS support
2) Always Keep PHP& MySQL updated
3) XSS, SQL injection, Session Hijacking and CSRF filtering
4) Use shared authentication with token
5) Use the advanced Password policy (Expiring, password structure and extended password policy)

Question 6: Security measures taken by company against the threats in cloud e-learning users

DoceboLMS supports the various kinds of authentication methods to keep the users to secure from various security threats. They are Kerberos and NTLM based authentication, REST API based authentication, POST/access Token based authentication and POST based authentication.
**Question 7: Security measures taken by company to protect the e-learning materials and other information in their system**

Docebo concerns information security as high priority on all of their products and services. So they follow many security measures to handle the various vulnerabilities over client’s information which used over their Cloud E-Learning system. They are:

1) DoceboLMS Cloud E-Learning platform is designed to install on customers or any third party datacentre, which allows the clients to choose the datacentre which they feels to be safe for their organisation.

2) Perform daily backup to keep the database and other files to be safe from any security vulnerabilities. And also allows remote backup facility.

3) Docebo provides the wide range of support for their clients to ensure the information security with remote bug fixing, software upgrade and software maintenance.

(Docebo, *DoceboLMS Features*, 2011)

**4.3.3 Cloud E-Learning Company “Blackboard Learn - ANGEL”**

**Question 1: Company’s profile**

Blackboard Inc. is a leading USA based E-Learning solution provider who have worldwide braches in many countries like Canada, china, Australia, UK, Netherlands. Blackboard Inc. has the wide range of E-Learning market throughout world, where it offers their services to Higher education institutes, K-12, Government sectors, Military, and Corporations. Blackboard Inc. has worldwide clients from man countries, some of the prestigious clients are Cedar Creek, CSI Global Education Inc., American Oil Chemists’ Society (AOCS), and CHICA – Canada. (Blackboard, *Association Clients*, 2011)

**Question 2: Products & services offering to customers**

Blackboard Inc. offers many E-Learning products and services to many institutions and Universities throughout world. Some of the blackboard’s e-learning products and services are Blackboard Learn+, Blackboard Collaborate, Blackboard Connect, Blackboard Analytics, Blackboard Mobile, and Blackboard Transact. In the year May 2009, ANGEL LMS is acquired by the Blackboard Inc. and they keep this E-Learning solution under their exciting Blackboard Learn+ product. (Blackboard, *About Bb*, 2011)

**Question 3: Are you own your server for your products and services? If not, you have full access for your outsourced servers?**

Blackboard ANGEL LMS is powered and hosted by ANGEL network servers which are located in Indianapolis, Indiana. ANGEL network datacenter servers are restricted to access by minimal list of authorized personnel who have access to sensitive areas and equipment. (ANGEL_LEARNING, *Application Hosting Services*, 2011)
Question 4: Security management standards taken against security threats on their products

Blackboard ANGEL LMS is driven by the standard based approach to its product development as an open system, which helps to simplify the integrations and keep the total cost of ownership to be low. So, Blackboard ANGEL LMS is certified and member of many security management standards, such like as member of IMS Global Learning Consortium (GLC) Contributing, member of Schools Interoperability Framework (SIF), and certified by ADL SCORM Certification. (ANGEL_LEARNING, Standards Leadership, 2011)

Question 5: Security measures taken by company against server security threats

Blackboard ANGEL LMS is powered and hosted by ANGEL network servers, which is protected by many advanced security measures to keep it safe from various server security threats. They are (ANGEL_LEARNING, Application Hosting Services, 2011):

1) Servers are secured by many physical security measures like biometric hand scanners, iris scanners and digital cardkey access which provide the multiple levels of protection from the unauthorized access. And finally all the server locations are monitored by digital cameras to record the all the activities inside and outside of datacentre’s location.

2) All the servers are powered with uninterruptible power supply with the help of three industrial grade UPS systems and also a 1500KW diesel generator. These backup power supplies are helps to run the servers and maintaining uninterrupted power in the event of surges or outages.

3) Data centres are always maintained with well air conditioning and air handling to avoid overheating of the servers. These climate controls are achieved with the help by state of the art HVAC (Heating, ventilation, and Air Conditioning) units. These systems are helps to maintain the constant airflow and precisely controlled temperature and humidity settings.

4) An advanced microprocessor and interrupt-based communications systems are used to detect the fires in the location of datacentre.

5) Blackboard ANGEL network data centre is uses the three OC-3 connections with a capable of 155 Mbps to UUNet, SBC, and US signal. This surplus OC-3 connectivity is also used for BGP routing, which helps in the time of an outage to instant traffic rerouting.

Question 6: Security measures taken by company against the threats in cloud e-learning users

Blackboard ANGEL LMS is follows many security mechanisms and security measures to keep the users of their E-Learning suite and their valuable information in the E-Learning system to be safe from various threats. They are (ANGEL_LEARNING, Technology and Systems Integration, 2011):

2) The security infrastructure of the Blackboard ANGEL LMS can be customized with the help of adapters in the case of migration to other security mechanisms, which is already followed by client's institution/organization.

3) Blackboard ANGEL LMS has already been integrated successfully into the Shibboleth authentication & authorization framework.

4) Blackboard ANGEL LMS can be able to run using SSL, for to encrypt important data as it is transmitted.

Question 7: Security measures taken by company to protect the e-learning materials and other information in their system

Blackboard ANGEL LMS follows many advanced security measures to keep the information stored in their servers and E-learning suite of the users to be secured from various threats. They are (ANGEL_LEARNING, Application Hosting Services, 2011):

1) Blackboard ANGEL Servers are monitored around the clock with well experienced technical staff from the Blackboard Inc. for 24/7/365.

2) AHS Watchdogs keep constant performance monitoring and troubleshooting on the servers which helps to ensure the peak performance.

3) Servers are protected with high secure mechanisms with the help of real time backup and daily off-site storage, which assures that the data stored in servers are secure.

4) Software’s stored in Blackboard ANGEL servers are regularly updated. So clients need not to worry about the software installation, upgrades and maintenance of their ANGEL LMS instance. Latest software upgrades and patches ensure that the information is secure.
5 ANALYSIS AND RESULT

This section is to analyse our results of theoretical and empirical findings in comparative way to bring the result for our research questions of the study. For that, all the vital points which are collected in theoretical and empirical findings are analysed and compared with each other to find the similarities and differences with them for our research questions of this thesis.

RQ1. Server security in cloud based e-learning:

Results from the theoretical study suggested and proposed many server security measures which help to avoid the threats against servers that run the cloud based e-learning solutions. In that, some of the key security measures explained the way about how to protect the servers from various physical threats. The results also explained the management standards which ensure the server security in cloud based e-learning technology. And further the theoretical study shows the importance of authentication to protect the servers from intrusion of hackers.

In the empirical study, from the results obtained from three different cloud based e-learning solution vendors, found the key server security measures which are used to protect their servers. Among the key security measures, physical security is one of the important measures considered by all the three companies to protect their data centres from various physical threats. Apart from that, the companies are using high-end technologies in their data centres to provide the uninterrupted power supply to their servers along with high speed data transmission from their servers. Finally, all the three companies are using various authentication methods to ensure the server security.

Comparison between the theoretical and empirical results uncovers some similarities between them in the cases of physical security and authentication methods. These similarities prove that the companies strictly follow the latest trends to protect their cloud based e-learning servers from various vulnerabilities.
RQ2. E-learners security in cloud based e-learning:

From the theoretical study, we get some key security measures which help to protect the E-Learners in cloud based E-Learning technology. These include various security mechanisms, security certificates, security management standards, encryption methods. The security measures help to provide the psychological confidence level to the e-learners on their safety to use the cloud based e-learning solutions. Apart from these security measures, theoretical findings also help to know some key security threats on e-learners in cloud based e-learning technology, such as browsers security, user authorization and authentication.

From the empirical study, we understand the various security measures and techniques followed by companies to ensure their customers safety from the vulnerabilities and attacks in cloud based e-learning technology. Some of the measures followed by three
companies include inbuilt virus scanners to scan and clean the virus/malwares from their servers to customer systems or vice versa, various password protection policies and authentication methods to avoid the intrusion into their cloud servers.

Comparative analysis on both theoretical and empirical studies shows the similarities between both of them on providing the security to the e-learners in cloud based e-learning technology. Some of the similarities are strong password policies and authentication methods which are used to protect the e-learners from security threats.

![Diagram of E-Learners security in cloud based E-Learning](image)

**Figure 14: E-Learners security in cloud based E-Learning - Key results of Theoretical and Empirical study**

**RQ3. E-learning materials security in cloud based e-learning:**

The theoretical study revealed the key security measures and security management standards which are used to protect the information in cloud based E-Learning technology from various attacks. Apart from that, it also stated the importance of security in the events of
incomplete data deletion and data lock-in that makes the information stored in CBE solutions vulnerable to external sources.

The empirical study also throws light on the key security measures like frequent backup and updates, improved password policies, secure authentication methods and security certificates used over CBE solutions to ensure information security. It also mentioned about various security management standards like SCORM, ISO and IMS used by CBE companies for to secure the E-Learning materials used over in CBE solutions.

Comparative analysis of theoretical and empirical study shows the similarity of outcome on the E-Learning materials security in CBE technology. Some of the similar solutions obtained are management standards that are used to ensure the information security, authentication methods and policies used to protect the unauthorized access over information stored in CBE solutions.

Figure 15: E-Learning materials security in cloud based E-Learning - Key results of Theoretical and Empirical study
6 DISCUSSION

6.1 CONCLUSION

From our research studies, we found many useful security measures which are being used to handle various security threats over cloud based e-learning technology.

Security is much important than any other issues in cloud based e-learning:

First issue is why is the security so essential in cloud based e-learning? As mentioned in section 3.9, the figure 10 shows that the security is very important concern for using cloud sources for any kind of technology. If the security concerns of the customers are not satisfied, it leads to psychological distraction in users’ mind about the specific product or technology. So, customers do not like to use the technology or product leading to its application failure.

Cloud computing provide more provisions to traditional E-Learning technology:

Next issue is why the cloud technology is to be used in traditional e-learning technology? As described in section 3.6 to 3.8, the cloud computing helps to bring more efficiency than traditional e-learning. Various advantages in using cloud technology to enhance the traditional e-learning technology are also explained (see section 3.8.2).

Finally, our research results answers the main research question of the study: “What can be the key security issues in use cloud computing for e-learning systems?” When we made a comparative analysis of theoretical and empirical studies on this, we found some key security issues over cloud based e-learning technology; which are listed below:

- **Cloud based e-learning technology is safe to use:**
  Section 3.10 shows various security threats and vulnerabilities over cloud based e-learning technology and its users, servers, and information’s. But these threats are frequently overcome by countermeasures taken by cloud based e-learning solution vendors.

- **Security management standards are helps to ensure the safety in mindset of CBE users:**
  Our theoretical study shows that various security management standards (see section 3.11) are used to ensure the security of CBE technology. These management standards help to raise the positive mindset on the customers to use the CBE technology and its products without any fear over its security. And also our theoretical as well as empirical study show that various security measures are used to overcome the security threats in CBE technology.

- **CBE solution vendors are more conscious about security issues in CBET:**
  Our empirical study results show that all the cloud based e-learning solution vendors are conscious about the security threats of this technology. It shows that they are using various security measures and security management standards to overcome these threats. They also conducting frequent security test programs to their products for to ensure stability against latest security threats of this technology.
Specific Results:

Apart from our general results of the study, we also gave more specific results on our sub research question separately. Those results are as follows:

**RQ 1:** What can be the Server security issues in cloud based e-learning?

As mentioned in fifth chapter, server security is ensured with various security management standards and security measures by CBE technology over various security threats. Physical security of cloud servers is ensured by various security methods and techniques. Frequent backup helps to provide additional safety for the data on servers. So server security is satisfied in cloud based e-learning.

**RQ 2:** What can be the E-learners security issues in cloud based e-learning?

Again the fifth chapter shows that various security measures and management standards ensure the e-learners security in CBE from various threats. Various security mechanisms used in CBE shows the protection of client side data and security of their machine. Various authentication methods are used ensuring the protection against intruders over CBE products and their users.

**RQ 3:** What can be the E-learning materials security issues in cloud based e-learning?

The analysis of results from theoretical and empirical studies in fifth chapter shows that the various security management standards are in use to ensure the data security in CBE from various threats. SCROM, ISO, IMS are some of the key security management standards which are accepted by many CBE solution vendors and implementing these standards over their CBE products for to provide better data security to their customers. Apart from these security management standards, many security methods and techniques are adapted to overcome the threats over data storage in CBE products.

### 6.2 IMPLICATIONS FOR INFORMATICS

In the book called “The book of informatics” by (Gammack et al., 2006) mentioned that informatics is a field which covers various academic fields related to information. So, Informatics deals with the field of information systems which include the development and maintenance of data stored in information systems. The security plays the vital role in a field of information systems where the maintenance of data is crucial. The results gained from our study are used to explore the security issues in cloud based e-learning technology. These results help to understand the security issues in cloud technology and its integration with e-learning field. Information systems can be better off in future in the security field by implementation of these results with cloud sources on any existing technology. Additionally our thesis results implicate the informatics to bring more security developments on upcoming information systems which come along with the cloud power.
6.3 METHOD EVALUATION

Text analysis is used as a method of evaluation for our study, as this analysis is having an advantage to analyse the information from various subject areas and relate the same to our research area i.e. security issues in cloud based e-learning. Text analysis also helps to analyse the previous research with respect to our research questions. We collected various articles on our subject area and analysed these materials with various other article results. Finally, reliable results are obtained as answers to our research questions.

After completion of the theoretical study, we used empirical studies to crosscheck our findings. In empirical study, we used three cloud based e-learning solution vendor’s websites as our sampling for empirical research. All these companies published their product details clearly on their websites. So we took the answers for our questionnaires from the published data of those websites. Subsequently text analysis is used once again to analyse the procured data from websites. These final results helped us to strengthen our theoretical results and ultimately paved more reliable resolutions based on this validation.

In the final analysis, constant comparison method is used to analyse our results from theoretical and empirical studies. This comparison technique helped to bring out the key security issues in cloud based e-learning including various factors like server security, e-learners security, and information security. The results of our analysis are presented in pictorial format.

6.4 RESULT EVALUATION

Our thesis purpose is to analyse the various security issues in cloud based e-learning. Data analysis is used on various research articles to obtain theoretical results for our research questions. As mentioned in section 2.5, we applied four different evaluation methods on our thesis results. They are quality, validity, reliability, and generalizability.

At first, the quality criteria are applied by constant evaluation on our theoretical and empirical findings. If the results are tampered at any place, it affects the overall quality of results. Strict analysis on the research articles will extracts only the good valuable points which relates to our subject areas. Before that the subject areas are chosen on the basis of get quality output for our research questions. The empirical study results are collected through the analysis of the websites of three of the world’s best cloud based e-learning solution vendors. So the empirical findings from those vendors really gave quality output for our research question.

Also the validity criteria for our thesis results are found through by the reliable empirical findings from the websites of various cloud based e-learning solution vendors. It is must to have the valid result which ensures the theoretical and empirical findings are related to each other and not having much more gaps between them. This implicates literally matching of results from articles with reality results. In our thesis, the results from empirical findings ensure that the companies are following our theoretical findings in real world environment. This shows the validity of our research results for this dissertation.
The reliability criteria of our thesis results are consistent through the conscious selection of research articles in finding answers to our research questions. We selected and reviewed as many research articles to perfect theoretical study for our study. Those articles are collected through various sources like IEEE explorer, Google scholar, LIBRIS, etc. In general IEEE articles are considered as reliable source, so we mostly gave priority to IEEE articles than any other sources. And apart from this, companies we chosen for our empirical study are world famous cloud based e-learning solution vendors. So the results from the websites of those vendor’s will surely bring the reliable outcome to our research questions.

Finally, the generalizability criteria of our thesis results are explained in detail on section 6.5.

6.5 POSSIBILITIES TO GENERALIZE

This section is for explaining the possibilities to generalize our thesis results, which also used to explore the validity of our results apart from the sampled selection for the research study. Theoretical results show the key security measures and management standards used to overcome the security threats in cloud based e-learning technology. And also the theoretical results are basically gathered through our subject areas. Those subject areas deals with cloud computing and e-learning field separately in order to get results for cloud based e-learning technology. These results have implications to generalize the research study on other cloud based technologies. For e.g. server security issues found through our theoretical study are also applicable for other cloud based technologies, because the server security completely depends on the cloud computing. So those results are applicable to any technology that uses cloud servers as their primary data centre. But almost all our results are only specific to cloud based e-learning and its security issues, so the overall result may vary to an extent for other cloud based technologies.

The empirical study results are acquired with the help of cloud based e-learning solution vendors from various regions of the world. The questions used in our empirical study are closed to security issues in CBET. So that empirical study may use to generalize to other issues in CBE with the help of wide range of cloud based e-learning solution vendors and also with the different questions which seeks the answers for other issues presented in CBET.

6.6 IDEAS FOR CONTINUED RESEARCH

Our study fully focused on the security issues in cloud based e-learning technology. But as mentioned in section 3.8.3, there are some other limitations in CBE technology. So people may continue to work on our research limitations presented in CBE technology. That kind of research will imply to bring more powerful and effective CBE products. Apart from this, our research will found to be useful in mobile e-learning technology as there are security issues in mobile technologies too.
6.7 SPECULATIONS FOR THE FUTURE

Security is the major concern for the customers in any technology when it comes to IT market. Many organisations and institutions are working to bring the effective ways, to overcome security threats in those technologies. The results of our study may vary in future when applied to new hacking techniques or other vulnerabilities. So our research work needs to be revised and updated in future, for to bring the new results in solving those security issues of CBE technology.
7 BIBLIOGRAPHY


OATES, B. J. 2006. Researching information systems and computing, Sage Publications Ltd.


# 8 APPENDICES

**Appendix 1:** Questionnaire used to understand the profile of CBE service vendors

<table>
<thead>
<tr>
<th>Company’s Background</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Questions</strong></td>
<td><strong>Response</strong></td>
</tr>
<tr>
<td>What is company’s legal name?</td>
<td></td>
</tr>
<tr>
<td>When was your company founded?</td>
<td></td>
</tr>
<tr>
<td>Where is your company located?</td>
<td></td>
</tr>
<tr>
<td>Who are all the customers of your company?</td>
<td></td>
</tr>
<tr>
<td>What are all the products and services offered by your company?</td>
<td></td>
</tr>
<tr>
<td>Is your company using your own data center for all your CBE products and services? (yes/no)</td>
<td></td>
</tr>
<tr>
<td>Do you have full access on your 3rd party data center? (Leave this question, if you mention yes for above question)</td>
<td></td>
</tr>
<tr>
<td>Where your cloud server is located?</td>
<td></td>
</tr>
</tbody>
</table>

**Appendix 2:** Questionnaire used to understand the Server security issues in CBE

<table>
<thead>
<tr>
<th>Server security issues</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Questions</strong></td>
<td><strong>Response</strong></td>
</tr>
<tr>
<td>What are all the physical security measures taken by your company on your Cloud servers?</td>
<td></td>
</tr>
<tr>
<td>What are all the server security mechanisms handled by your company against server security threats?</td>
<td></td>
</tr>
<tr>
<td>What are all the security management standards using by your company to ensure the security of your servers?</td>
<td></td>
</tr>
</tbody>
</table>

**Appendix 3:** Questionnaire used to understand the E-Learners security issues in CBE

<table>
<thead>
<tr>
<th>E-Learners security issues</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Questions</strong></td>
<td><strong>Response</strong></td>
</tr>
<tr>
<td>What are all the security measures taken by your company against E-Learners security threats?</td>
<td></td>
</tr>
<tr>
<td>What are all the security management standards using by your company to ensure the security of your customers?</td>
<td></td>
</tr>
<tr>
<td>What are all the authentication mechanisms</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 4: Questionnaire used to understand the Information security issues in CBE

<table>
<thead>
<tr>
<th>Information security issues</th>
<th>Questions</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What are all the security measures taken by your company against information security threats?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is your company providing backup/restore facility to protect the information?</td>
<td></td>
</tr>
</tbody>
</table>
University of Borås is a modern university in the city center. We give courses in business administration and informatics, library and information science, fashion and textiles, behavioral sciences and teacher education, engineering and health sciences.

In the School of Business and Informatics (IDA), we have focused on the students' future needs. Therefore we have created programs in which employability is a key word. Subject integration and contextualization are other important concepts. The department has a closeness, both between students and teachers as well as between industry and education.

Our courses in business administration give students the opportunity to learn more about different businesses and governments and how governance and organization of these activities take place. They may also learn about society development and organizations' adaptation to the outside world. They have the opportunity to improve their ability to analyze, develop and control activities, whether they want to engage in auditing, management or marketing.

Among our IT courses, there's always something for those who want to design the future of IT-based communications, analyze the needs and demands on organizations' information to design their content structures, integrating IT and business development, developing their ability to analyze and design business processes or focus on programming and development of good use of IT in enterprises and organizations.

The research in the school is well recognized and oriented towards professionalism as well as design and development. The overall research profile is Business-IT-Services which combine knowledge and skills in informatics as well as in business administration. The research is profession-oriented, which is reflected in the research, in many cases conducted on action research-based grounds, with businesses and government organizations at local, national and international arenas. The research design and professional orientation is manifested also in Innovation Lab, which is the department's and university's unit for research-supporting system development.