CHAPTER II

2.1 INTRODUCTION

Nowadays the education depends widely on the technology; the technology has vital impact of the modern education. It is necessity to use the technology at the university classrooms, utilizing the technology give the lecturers the power to show more data to their students and help to enhance the students learning. The use of different technologies in the classrooms save the time and help the students to understand exactly what the lecturer attempting to say, and take into consideration more attention to be paid to the content of course (Alkhateeb et al., 2010).

Technology is a critical instrument in applying and ensuring the successful e-learning. As being defined, e-learning means having people talking, composing, teaching and learning with each other online or in other words, utilizing computer-based systems. E-learning is discovered for the most part with a suitable software apparatuses. E-learning encompasses any correspondence available to members from any email, talk board, web journals, face book, twitter and other related technology that help e-learning. Including the increments of mobile technology and new tablets of technology, for example, iPod and iPhone could contribute the easiest methods for implementing e-learning. The technologies additionally contribute effectiveness at teaching in the class and encourage the exploration of knowledge in different ways (Yacob et al., 2012).

2.2 E-LEARNING

E-learning facilitates and enhances the learning process through the use of devices based on computer and correspondences technology. E-learning covers a general category of uses and processes, for example, education through the Internet/Intranet (web based learning), education provided by computer (computer based learning), virtual classrooms and advanced joint effort. The content is offered electronically through the Internet, Intranet, sound or video tapes, satellite, Disc ROM or DVD. Typically the e-learning term is understood as online education (web based learning) and online courses. Considering this aspect, the computer based learning process can be seen as an e-learning component which does not require a nonstop interaction with a teacher and other students (Luminita, 2011).

2.2.1 The Development of E-Learning

The upheaval in the data and correspondence innovation, direct straightforwardly to the development of the e-learning, also it is diminishing the expenses. The force of data and correspondence engineering is in supporting the interactive media (Gambhir, 2008). The development of e-learning is specifically identified with the expanding access to data and interchanges in engineering; also it is diminishing the expense.

Through the comparison of the indices used in e-learning readiness models made by (Darab & Montazer, 2011), it is mentioned that preparation, content availability, social status and budgetary assets are consistently accentuated in most of the models instructive standards, or only few have accentuated on instructive approaches. Likewise, having distinguished those components that help the formation of the virtual instructive environment and merging them with the rule files of e-learning in status,

little uncertainty remains important to create a fitting appraisal model to be used in securing the level of e-learning in availability of the Iranian higher training associations. The model produced as in Figure 2.1 will be the guide for researcher's study.

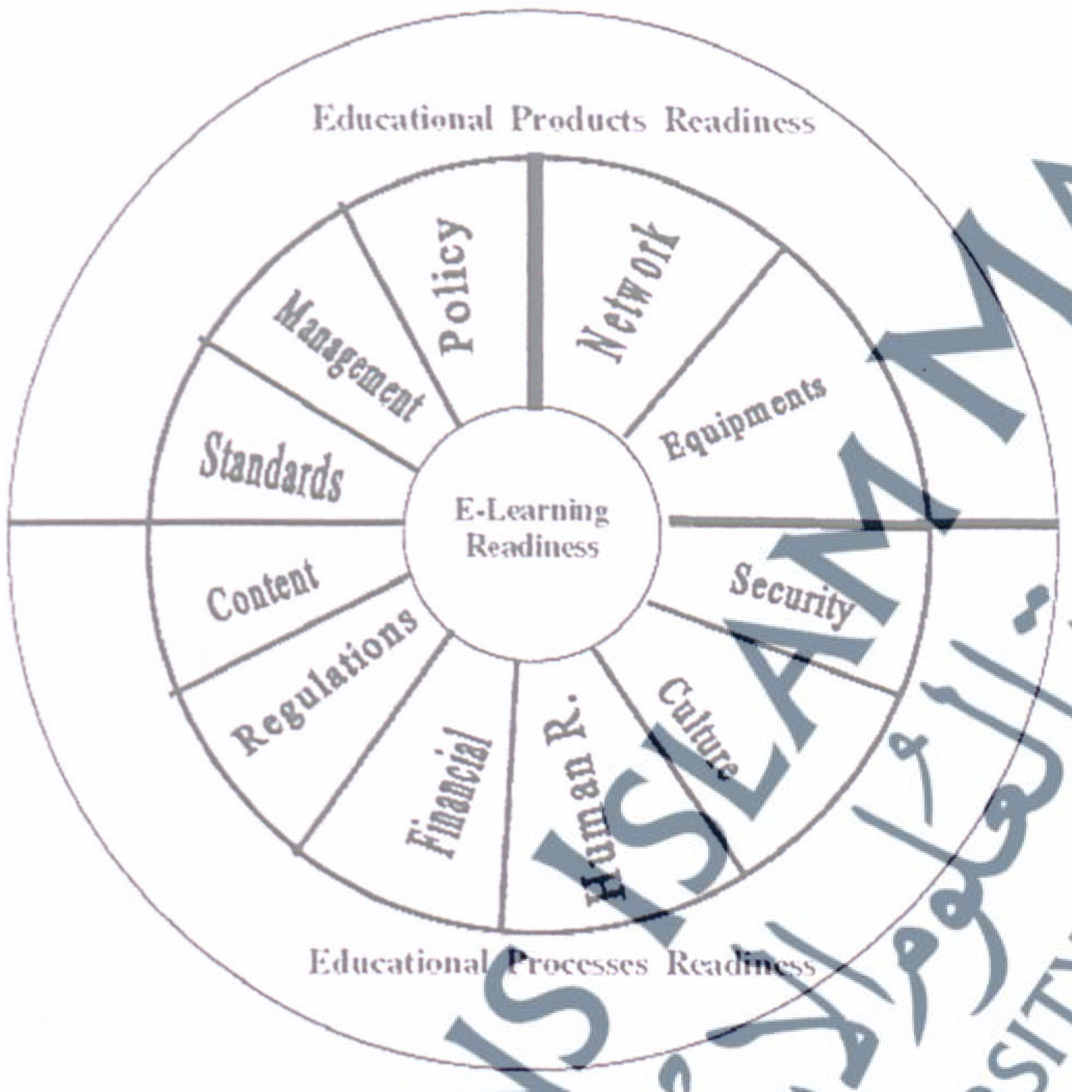

Figure 2.1: E-Learning Readiness Model (Darab&Montazer, 2011)

2.2.2 Challenges in E-Learning

Implementing e-learning is not an easy task. Despite many benefit gained from e-learning, there are also issues and challenges when aiming to make e-learning successful.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA
جامعة العلوم الإسلامية الماليزية

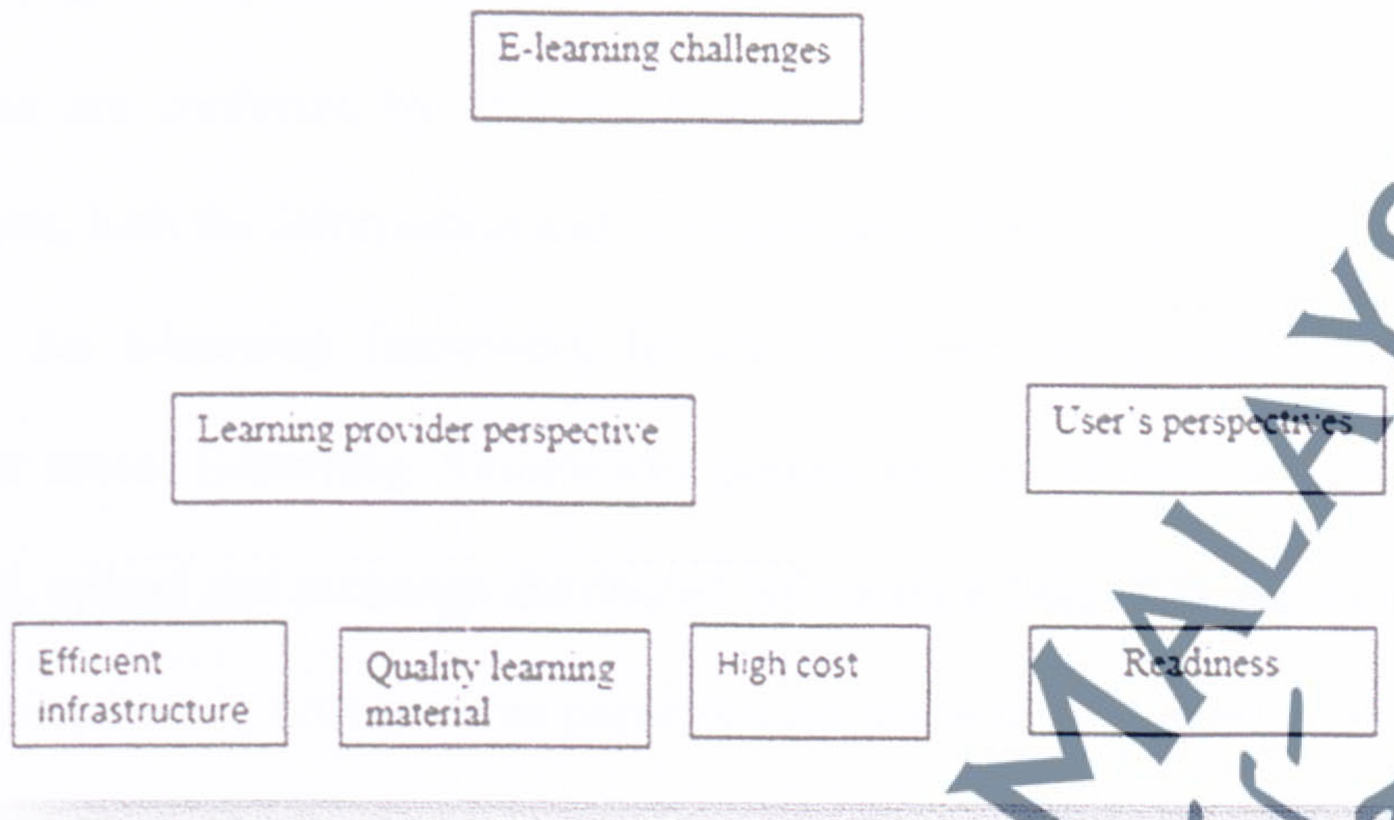

Figure 2.2: The E-Learning Challenges (Source: Alwi & Fan, 2010)

The challenges, as reflected in Figure 2.2, are considered from two points of view: the learning supplier, and the client. From the learning supplier point of view, Higher Learning Institutions (HLIs) are encountering troubles in relation to various technological issues, for example, efficient infrastructure, where students will be dependent on these facilities to access to educational material on the Internet. Moreover, the delivery of high bandwidth content, such as digital video, is still problematic to the home user. Learning material is also an issue, since a lack of quality content is prepared. Developing good content for students should consider many different factors, such as pedagogical aspects, human-computer interface, and expertise. Ensuring all of these are well-prepared requires a high budget; thus, high costs for implementation are to be expected. In a developing country, all of these challenges are even more difficult, simply because of the resources issues faced (Alwi & Fan, 2010).

2.3 E-LEARNING SECURITY

Ahmed et al, (2011) mentioned that e-learning is the procedure where learning and instruction are conferred by utilizing a wide range of electronically empowered innovations, both the Information and correspondence frameworks directed to give e-learning. An e-learning framework for the most part is spotted consistently in numerous areas. E-learning frameworks permit various clients or applications to download, upload and exchange distributed information from different location of the world. Ahmed et al., (2011) in his paper discuss some of the issues in an e-learning and this paper support the problem statement of researcher's research.

Costinela-Luminita & Nicoleta-Magdalena (2012) discussed the improvement of the e-learning frameworks ought to be carried out utilizing universally perceived techniques and security norms. The framework needs to execute security administrations, for example, confirmation, encryption, access control, overseeing clients and their authorizations. The information exchange between the framework and heads or substance administrators ought to be carried out on encoded SSL channels through the web organization interface. A safe learning stage ought to join all the parts of security and make the vast majority of the methods more straightforward to the teacher and the student. Costinela-Luminitaand Nicoleta-Magdalena(2012), In their paper discussed the typical threats of e-learning systems and how we can address these issues. It also discussed the security and privacy vulnerabilities of the most popular open-source e-learning systems, Moodle. This article supports problem statement in researcher's research.

Today web is the most famous and shabby wellspring of correspondence all through the world. Presently People have the entrance to web, from home, office, and versatile. Web have advantages and also disadvantages. The primary peculiarity that is security with ease, however, with the progression of time a considerable measure of different issues have been confronted by the web, that are concerned to speed and reliability (Jalal & Zeb, 2008).

E-learning is primarily dependent on data and in addition correspondence technologies. As per Rosenberg (2001), e-learning is based on three fundamental criteria, which are:

a) Network-capable upgrading, storage/retrieval, dissemination and imparting of data.
b) Delivery to the end of user by means of computer utilizing standard Internet technology.
c) Concentrate on the broadest view of e-learning.

The main and second criteria expose the e-learning. The principal and second criteria expose the e-learning establishments to the threats, as the use of ICT could ultimately lead to numerous possible data security dangers which could compromise data, for example, loss of confidentiality, accessibility, exposure of basic information, and vandalism of open data services. Unfortunately, very few efforts have been made to correct this circumstance. More endeavors have been underlined to improve the substance and engineering due to addressing content and innovation as the difficulties in securing a fruitful e-learning environment.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

Srivasta and Sinha (2013) discussed that security is required inside e-learning situations owing to the way that, these days, information has turned an important means of production, as product and as a key for individual achievement. In e-learning, data getting from helpful information is among the principle resources of the association. Among security issues in e-learning are insurance against control (students, insider), client validation, and secrecy. However, as the usefulness of e-learning is expanding, data must be actively protected in this bigger context to evade the loss of its confidentiality, integrity and accessibility. Some people may state that knowledge ought to be shared, however there are circumstances where the stream of sensitive data ought to be restricted to just a few well-defined gatherings, for example, learning materials for certain gatherings and copyright protection of intellectual properties. Srivastava and Sinha (2013) in his paper presented virtual training environment and its importance for the students as well as the whole society. This paper supports problem statement of researcher's research.

Some of associations and organizations are moving towards the e-learning methodology, the security issue turns into a huge test. This test and works out another component to actualize security demonstrating for e-learning. Under this new security demonstrating, e-learning frameworks can be better actualized by all stakeholders. At the point when e-learning frameworks are required for instructive organizations, there are diverse stakeholders/invested individuals included, in the same way as engineers, establishments, controllers, educators, organization staff, supporting professionals, learners. It is vital to characterize the security parts and important traits of all stakeholders separately. Security credits, which are applicable to all e-learning stakeholders, controller, foundation, designer, teacher, organization staff, educator and

learners. A security displaying for e-learning framework delineates the connections among e-learning stakeholders. Educators are accountable for course creation and conveyance through e-learning framework. Organization staffs are accountable for organization capacities of e-learning framework, in the same way as understudy enrolments, and so on. Supporting specialists are accountable for keeping up e learning frameworks as the specialized backing. Learners are the individuals who use e-learning frameworks to direct their learning. As they are all e-learning framework clients, their security qualities rely on upon engineers, foundations, and controllers.

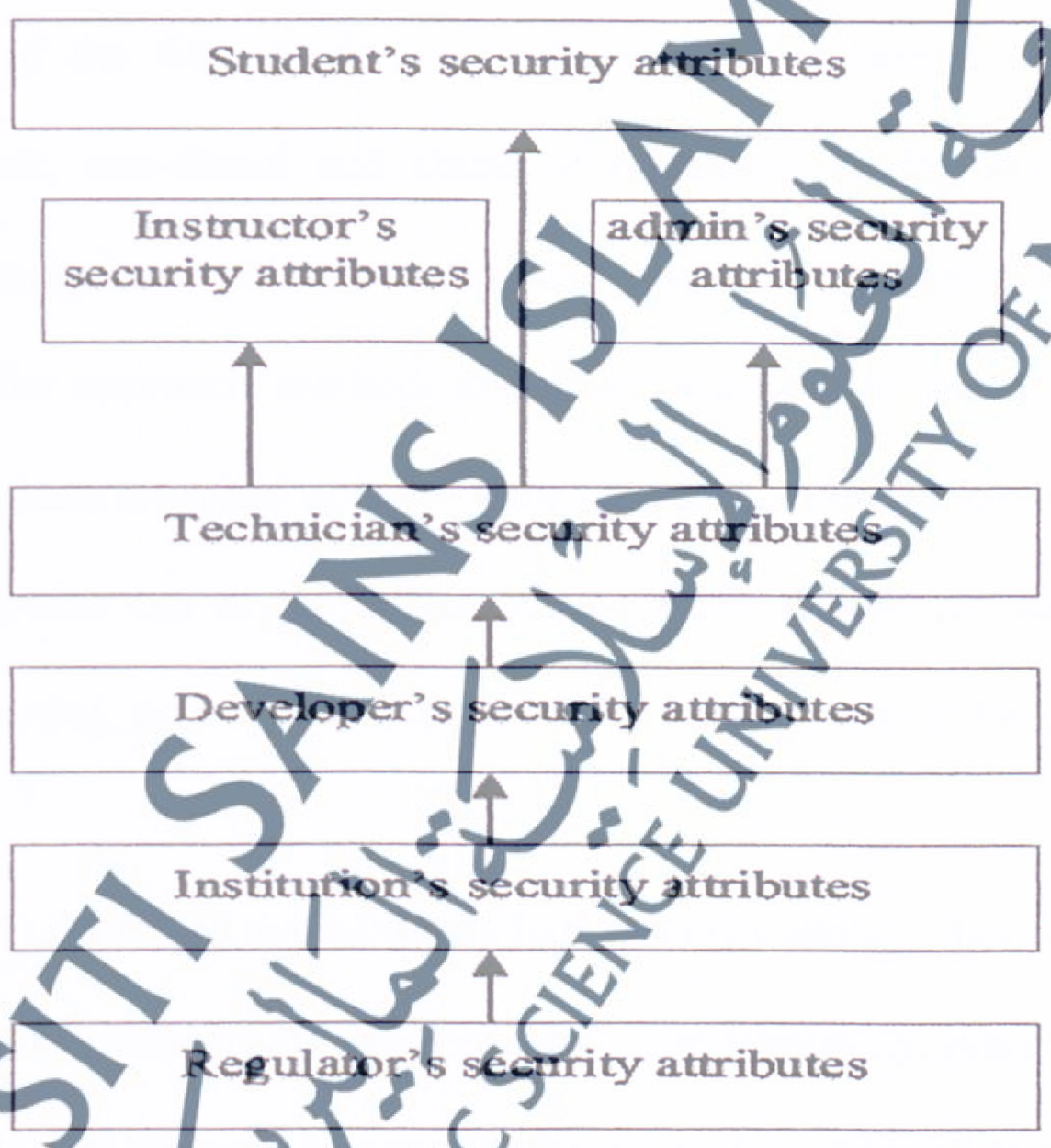

Figure 2.3: Security Modeling of E-Learning (Source: Yong, 2007)

Figure 2.3 illustrates the regulator's security attributes that will affect and influence the institution's security attributes. The institution's security attributes will affect and influence the security attributes of e-learning developers. The developer's security

attributes will affect and influence the security attributes of e-learning technicians. The technician' security attributes will affect and influence the security attributes of e-learning instructors, administration staff and learner. The instructor's security attributes and administration staff's security attributes will affect and influence the security attributes of e-learning learners (Yong, 2007).

2.3.1 Basic Security Requirements For E-Learning

E-learning is different from other e-services in the applications utilized; the methodology and the partner conduct molded nature in e-learning. Issues of dependability of the framework in course material, information security in the evaluating result, non-denial and abuse of e-learning (LMS) are case of social specialized security issue which is particularly identified with individuals. Individuals need to take after approach, methods and others exercises to guarantee the (CIA) is attained. Individuals are relied upon to be the security controllers themselves. However individuals likewise can be the vulnerabilities where danger can happen, for case: secret key imparting, non-denial, and malware infection (Alwi & Fan, 2012).

Luminita (2011) explained the following basic security aspects should be fulfill for e-learning platforms: authenticity, access control, confidentiality, integrity, availability, non-repudiation and privacy. A secure authentication is required to identify the user who will use the web application and to determine his access privileges. This mechanism prevents the attackers to access another user's account, to view sensitive information or to perform unauthorized operations. Also, once authenticated, the user should have the possibility to change his password. Luminita (2011), In this paper

discussed security assessment and this was related to in researcher's research objectives.

2.3.1.1 Access Control

Access control is a basic mechanism which aims at restricting accesses to shared resources to authorized entities only. Such restrictions contribute to the protection goals confidentiality, integrity, and availability by

- limiting read accesses contributes to confidentiality,
- limiting modifications contributes to integrity,
- allowing usage of resources only in a specified manner contributes to availability (Franz et al., 2006).

Access control - Users can't exchange or build the got benefits regardless of the fact that they team up without the culprit being recognized (Vasilescu et al., 2011).

2.3.1.2 Confidentiality

Due to the way that learning material by its tendency must be appropriated to the outside, industrial espionage and information robbery are not significant issues in e-learning. The client ought to get to the approved substance and those persons who are not the real clients should not have the capacity to get access to the system (Ahmed et al., 2011).

Confidentiality is where a client may wish to keep the substance of a message mystery from everything except the proposed beneficiary. It might likewise be essential that a

client keeps their personality, mystery from busybodies, so the privacy primary target is to keep LMS data from being uncovered to anybody not approved to get to it (Mohammad et al., 2012).

Confidentiality refers to keeping the revelation of data to unapproved people or systems. Because of the way that learning material by its temperament must be appropriated to the outside, industrial espionage and information robbery are not real issues in e-learning. In any case, in specific situations this is likewise of importance. Beside countermeasures against physical burglary of capacity gadgets, persevering security executives need to set up countermeasures against electronic robbery, for example, the establishment of firewalls and interruption discovery instruments to hamper assailants from the outside (Kim, 2013).

2.3.1.3 Integrity

Integrity is that just approved clients are permitted to alter the contents which incorporate creating, changing, appending and erasing information and metadata and the assaults on integrity are for the most part the endeavors made to effectively change or devastate data in the e-learning site without legitimate approval (Ahmed et al., 2011).

Mohammad et al, (2012) explained that Integrity measures are taken to protect information from transmission errors, however users might likewise wish to be protected from a message being changed deliberately for malignant reasons, additionally defines what rights and services the end user is allowed once server access is granted. Mohammad et al. (2012), in his research constructs a framework that can

be used to evaluate the security requirements of the Learning Management System (LMS), where the framework has four metrics; Availability, Confidentiality, Integrity and Authentication (ACIA) as key role in the security management of LMS associated with the e-learning and this paper supports problem statement in researcher's research.

Integrity - Modifications of transmitted or stored information must be detectable. In the event that reasoned by technical defects, adaptation to non-critical failure and error correction can be applied. In the event that reasoned by fraudulent usage, originator and context ought to be disclosed (Vasilescu et al., 2011).

2.3.1.4 Availability

Availability is a network service can be unavailable because of heavy movement conditions or hardware/software failures, yet a service can likewise be disrupted because of pernicious assaults that attempt to deny service (Mohammad et al., 2012).

Eswari (2011) mentioned that availability is ensuring that the information is available at any given time in order to access the courses or submit their assignments on time. Administration interims must be kept short and declared enough ahead of time. Disappointments, if any, ought to just prompt short interferences. Availability in e-learning is the confirmation that the e-learning environment is available by approved clients, at whatever point required. Two features of availability are normally talked about, which are dissent of administration and loss of information handling abilities. The e-learning clients are reliant on the data on the Internet; accordingly, the availability of the materials and data to be gotten whenever and wherever is urgent. In the event that, for instance, an e-learning stage is moderate, clients don't just oblige of

a chance time to do their work, yet they additionally get to be disappointed, expanding the negative impact on productivity. Neglecting to satisfy this will have a noteworthy effect on e-learning clients and e-learning suppliers. There are no compelling systems for the avoidance of dissent of administration, which is the inverse of availability. Then again, through perpetual observing of uses and system associations one can consequently identify when a denial-of-service attack occurs. Eswari (2011) addressed various security & privacy risks associated with e-Learning are enumerated and a process framework is proposed for securing an elearning ecosystem, which helps to address the security problem in a systematic way in order to foster the benefits of e-learning and this paper has relation with problem statement in researcher's research.

2.3.1.5 Non-Repudiation

Non-Repudiationis the last step in information security where the learner have to be provided with e-learning services without any possible fraud such as when computer systems are broken in to or infected with Trojan horses or viruses, to deny the works or changes done by them in the system (Luminita, 2011).

Non-Repudiation: guarantees that no gathering in an operation can deny partaking in the operation. We can likewise characterize the system of non-repudiation as the component concentrate on the way that the sender of the message can't deny having sent the message later on (Rjaibi et al., 2013).

2.3.1.6 Authentication

Authentication: a user may want to be sure that a received message was sent by the user whom they purport to be and not by someone masquerading as another.

Authentication involves validating the end users' identity prior to permit them server access (Mohammad et al., 2012).

Identification and Authentication: guaranteeing that the client is who he/she claim to be furthermore fitting access is allowed to the client. In an e-learning point of view just genuine learner or other distinguished partners of that environment ought to have admittance to the framework. Authorization: guaranteeing that the client has the power to get to the framework or data. In an e-learning point of view, the framework needs to guarantee that partners are permitted to get to those administrations for which they are approved (Eswari, 2011).

2.3.1.7 Privacy

Privacy: Is necessary to ensure non-disclosure of information given for each user. Privacy is required to ensure the security of information related to each user (Rjaibi et al., 2013).

E-learning framework security administration, privacy and access control are now pulling in all that much consideration because of the most recent patterns in training frameworks improvement and endeavor to make an electronic record of an understudy so as to empower the versatility of examining. Access control ought to anticipate unapproved access to imparted assets. Gathering such a prerequisite in e-learning frameworks is extremely mind boggling since it is important to ensure the substance, administrations and individual information not just from the outer clients of a framework, additionally from the advancement and managerial inward clients of a framework (Sabic & Azemovic, 2010).

2.3.2 E-Learning Vulnerabilities

Mu'azu and Lawal (2012) discussed that vulnerability is an attribute or quality of a component which can be utilized through both an external and internal agent (hacker or malicious insider) in order to breach a security policy or result in a dreadful result by either the segment itself, and the framework foundation of which it is a section. A hacker who threatens organization's information assets is taking advantage of vulnerabilities in the media and systems which handle them. Vulnerabilities and threats clearly go hand-in-hand: all threat is directed at vulnerability. This paper is related to security threat in researcher's research.

2.3.2.1 User Privacy Vulnerability

In e-learning, client security is additionally imperative since it can secure a fair situation. On the other hand, client security is defenseless because of operation and approach instrument utilized by e-learning. E-learning clients can't progressively sharpen their security from dangers utilizing namelessness in light of the fact that e-learning framework requires the information to enhance learning help. Actually, uncovering the client protection information in this setting is powerless against assault. It is because of assailants can sniff or take the information in transit (Derawi, 2014).

2.3.2.2 Content Vulnerability

One of the noteworthy issues in the e-learning space is content respectability. The ability to distinguish changes in learning substance has been smoldering for some applications. In this way, content verification has been a standout amongst the most imperative subjects in the e-learning world. Improperly, numerous e-learning frameworks don't offer the substance honesty assurance. Absolutely, they likewise

don't reflect advanced property right security to the e-learning substance. As a result, a true blue client of e-learning facilitates to abuse advanced property right of others by posting or TV the e-learning substance, for example course presentation files, tutorial video, software, and book, without approval (Derawi, 2014).

2.3.2.3 Web-based Application Vulnerability

The greatest amount of e-learning systems are web-based applications. As such, these frameworks likewise acquire all shortcomings of electronic applications. The online applications are powerless against numerous assaults due to; out updated security patch of web server, developer lacks in secure coding and increased interactive website(Atashzar et al., 2011).

Then again, expressed that electronic application, including e-learning, are defenseless against numerous assaults because of faint side of the web. The faint side of web can be separated into two gatherings, i.e., innovation driven and non-innovation driven. In the event of initially specified, then the assailant utilizes innovation in assaulting electronic application. In any case, assailant applies 'social designing' in misusing the shortcoming of clients for controlling electronic application. Spam, malware, hacking, disavowal of administration assaults, phishing, click extortion, and infringement of computerized property rights have been named innovation driven of the faint side of web. What's more, non-innovation driven incorporates online robbery, online tricks and fakes, physical mischief, digital tormenting, spreading untrue or private information, illegal online gambling, aiding crime and other reprehensible behaviors (Atashzar et al., 2011).

2.3.3 Risk Assessment in E-Learning

Lately, the issue of information security has become widely concern by organization that have long used information systems to perform their everyday operations. Risk management is performed through the procedure of identifying risks, assessing risks, and making moves to diminish risks to a worthy level (Lo & Chen, 2012).

Feng and Li (2011) explained that organizations are increasingly relying on Information Systems (IS) to improve business operations, encourage administration choice making, and deploy business strategies. The reliance has expanded in current business situations where a variety of transactions involving trading of goods and services are accomplished electronically. In practice, the ISS risk assessment is quite complex and full of the uncertainty as well. The uncertainty, existing in the process of assessment, has been the essential element that impacts the viability of the ISS risk assessment to a huge degree. Therefore, in order to deal with the incompleteness and vagueness of information, the vulnerability must be considered in the ISS risk assessment. Notwithstanding, most existing methodologies applied to the ISS assessment have a few disadvantages on handling uncertainty in the process of assessment. Feng & Li (2011), in this paper, proposed an ISS risk assessment model based on the improved evidence theory. Firstly, establish the ISS index system and quantify index weights, based on which the evidential diagram is constructed. To deal with the uncertain evidence found in the ISS risk assessment, his model provides a new way to define the basic belief assignment in fuzzy measure.

Generally speaking, several basic concepts such as risk, information system, information system security and risk evaluation are defined as follows:

- **Risk** is defined in ISO/IEC TR 13335-1 as "the potential that a given treat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets". And more concepts in relation with risk are also defined in ISO/IEC TR 13335-1. Defines security risk as referring to relative exposure of an information asset and the probability or likelihood that the asset can be compromised plus the possible loss. Risk can be translated as the formula below:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

It is established that the risk, threats and vulnerabilities are closely related and the relationship between them. The relationship model of these concepts, which makes a clear explanation to the relations of those concepts, is shown as Figure 2.4.

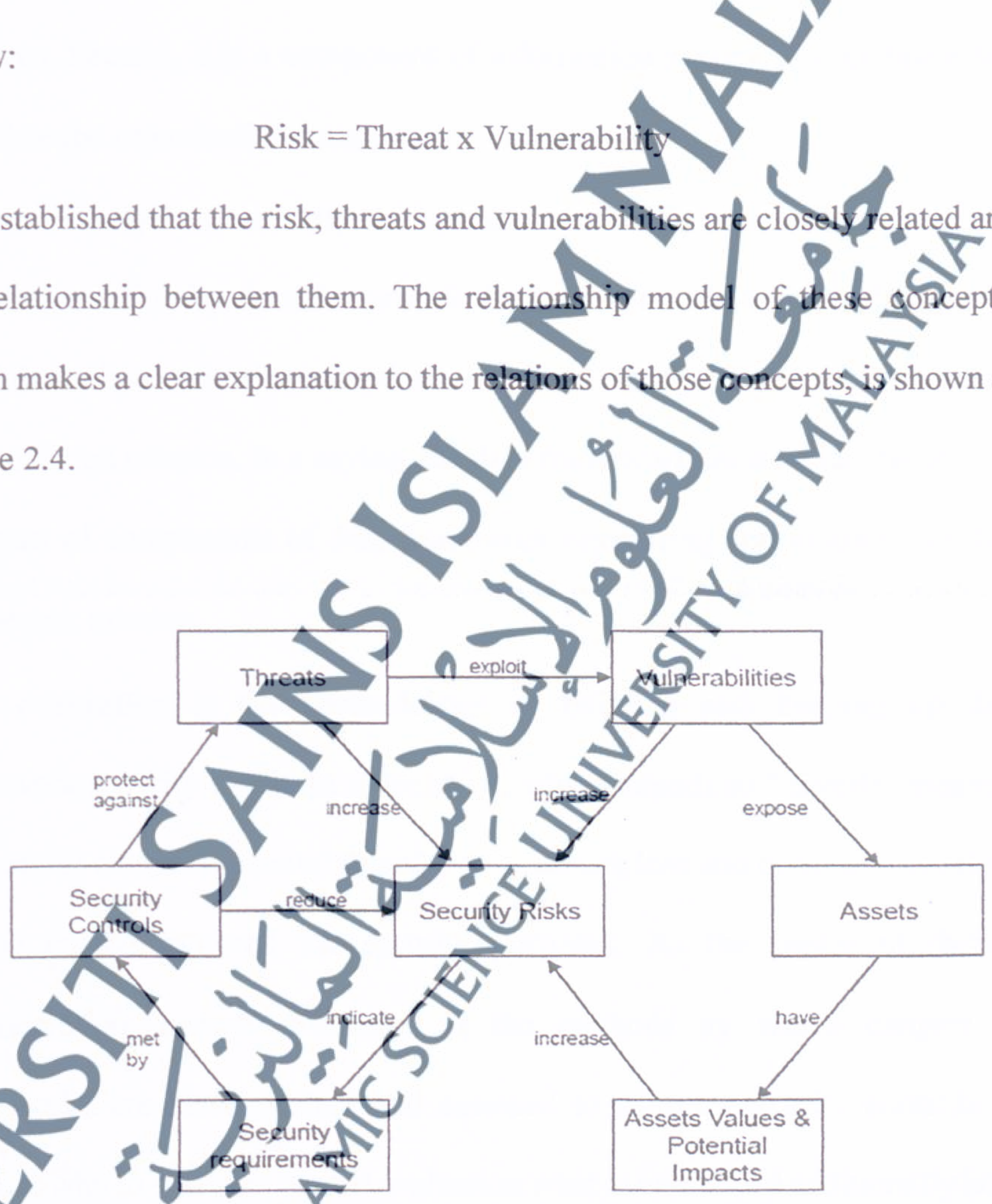

Figure 2.4: Relationships in Risk Management (Source: Zhiwei & Zhongyuan, 2012)

- **Information system** is a narrow concept of an information system, which refers to the computer-based system. It is an organic set of facilities as human beings, rules, databases, hardware and software, tools and running environment. It highlights the use of PC and system correspondence innovation. Two levels of implications are incorporated in the data framework. To start with, the capacity of data framework is to finish the association missions. Second, it is a component of information system to coordinate and complete the organization mission.
- **Information system security** is the reason for the information to finish the operation mission by data framework. In the meantime, the data framework depends on its constitution components and data during the time spent attaining to association mission. In a saying, the data framework security can be utilized as a part of components of data framework organizing and attaining to data framework mission.
- **Risk evaluation** is the methodology of building and keeping up data framework security inside an association, which intends to "identify, measure and control uncertain events" in order to minimize loss and optimize the return on the capital invested for security purposes. As the center of danger administration, hazard evaluation is the methods by which dangers to frameworks are distinguished and assessed to support security controls. It contains why to executes hazard evaluation what to assess and additionally how to assess on different issue. Zhiwei & Zhongyuan (2012), made detailed analysis from the purpose, the objective, the process methodology of risk evaluation according to the role, the structure and the environment of information system.

2.3.3.1 Security Threat Source

Threat intent represents the intent of the human who caused the threat:

- Intentional Threats: It speaks to dangers that are consequence of an unsafe choice. Case in point PC criminal acts, or when somebody deliberately harms property or data. Computer crimes include espionage, identity theft, child pornography, and credit card crime.
- Unintentional Threats: It represents threats that are presented without awareness. These dangers essentially incorporate the unapproved or incidental change of programming. Accidental error includes corruption of data caused by programming error, user or operator error.

A threat can be caused by internal, external or both external and internal entities.

A. **Internal threats:** Internal threats occur when somebody has authorized access to the network with either a record on a server or physical access to the system. A risk can be inward to the organization as the result of employee action or failure of an organization process.

B. **External threats:** External threats can emerge from people or organizations working outside of an organization. They don't have approved access to the PC systems or network. The most clear outside dangers to PC systems and the occupant information are characteristic catastrophes: hurricanes, fires, floods and earthquakes. External attacks occur through connected networks (wired and wireless), physical intrusion, or a partner network.

C. **Human Threats:** This class includes threats caused by human actions such as insiders or hackers which cause harm or risk in systems.

D. **Environmental factors:** Environmental threats are threats caused by non-human. It comes, in the first place, from common calamity dangers like quakes, surge, flame, lightning, wind or water and, likewise, because of creatures and natural life which cause serious harm to data systems like surges, lightning, Tidal Waves (like Tsunami) and fire. For sure, this class incorporates different dangers, for example, mobs, wars, and terrorist attacks

E. **Technological Threats:** Technological threats are created by physical and compound techniques on material. Physical processes include the utilization of physical intends to pick up entrance into limited regions, for example, building, compound room, or whatever other assigned range like burglary or harm of equipment and programming. In any case, synthetic methods incorporate equipment and programming advances. However, chemical processes include hardware and software technologies. It, also, includes indirect system support equipment like power supplies.

- **Threat motivation:** Attackers normally have a specific goal or motive for an attack on a system. These goals can cause malicious or non-malicious results.
- Malicious threats consist of inside or outside attacks caused by employees or non-employees to harm and disrupt an organization like viruses, Trojan horses, or worms.
- Non-malicious attacks occur due to poor security policies and controls that allow vulnerabilities and errors to take place. It is caused by ignorant employees with the aim not to harm the system.

Threat impacts: The security threat can cause one or several damaging impacts to systems. Which can be partitioned into seven sorts: Destruction of data, corruption of

data, theft or loss of data, disclosure of data, denial of use, elevation of privilege and illegal usage. Jouini et al. (2014) in this paper addresses different criteria of information system security risks classification and gave a review of most threats classification models. It also identified a hybrid model for information system security threat classification in order to propose a classification architecture that supports all threat classification principles and helps organizations implement their information security strategies. This paper supports the first objective in this research, that is to identify the information security threats faced by GOALS in USIM.

2.3.3.2 Security Threat Classification

A. Errors and omissions: Errors and omissions are dangers that influence information and system integrity. These errors have not just been created by information entrance clients, who process a high number of exchanges a day, yet they additionally are brought about by a wide range of clients who make and alter information. Now and then, mistakes are the dangers themselves, in the same way as a programming mistake or an information entrance blunder that crashes the system.

B. Fraud and theft: Both of fraud and theft are also information system security threats. They can be submitted in ways the conventional misrepresentation and robbery were conferred, while there are likewise some newer techniques. For instance, an employee can use the organization's information system to steal a small amount of money from different financial accounts. The stolen cash may not be checked furthermore is hard to be found because of its little sum. However, a large number of this type of thefts might eventually result in a large amount of loss. Sources of

computer fraud or theft can be both insiders and outsiders. Authorized users for the system are an example of insiders. The insiders include technical staff members and general users like general users.

C. Employee sabotage: Employees' deliberate actions such as mischief and sabotaging can also cause damages for the information system, because of the weaknesses of the computers and applications. So when they have negative feeling to their association or when they feel restless about their occupations, they can attack against their organization. Such as destroying hardware or facilities and destroying programs or data using planting logic bombs.

D. Loss of infrastructure that supports the system: Usually, this sort of dangers result in a system downtime, and it is frequently outside the ability to control of the holders of the data frameworks' assets. The loss of supporting foundation happens in circumstances, for example, fire, flood, power failures, loss of communications, etc.

E. Malicious hackers: This kind of dangers have quickly turned into an imperative part of the data system, as an aftereffect of the advancement of correspondence systems and the Internet. The term programmer portrays an unapproved individual who tries to separate the data system security, and who then may harm the data system, let the system insecure, change or take information, and/or lose data. Generally, a general harm created by programmers is much littler than that brought about by robbery or extortion, in light of the fact that the programmer's impact is typically littler. On the other hand, programmers' exercises nowadays have pulled in more considerations of data system security specialists.

F. Malicious code: This type of security threats includes viruses, Trojan horses, worms, logic bombs, and all "unwanted" software. The three most significant kinds of Malicious Codes are:

- **Viruses:** They are pieces of code which can copy themselves to executable software. This new duplicate can be executed when a client executes a system which the infection was appended to. It may do some sudden things when it meets a particular condition, in the same way as a period or a date. Case in point, it shows undesirable messages at a certain timing.
- **Trojan Horses:** They are a kind of projects that perform undesired sudden errands. For example, it may erase clients or adjust client bunches in a multiuser system. Additionally it may arbitrarily erase a document from the client's system.
- **Worms:** They are projects that repeat themselves and reduce the system execution. More often than not, worms utilize system's administrations to duplicate themselves to different hosts systems.

G. Threats to personal privacy: Because a vast amount of electronic personal information are stored in many different databases, which belong to different organizations, they has been a huge threat to individuals' privacy. These kinds of personal data can be used in many different undesired ways. Alhabeeb et al., (2010), the aim of his paper is to design a methodology that can classify deliberate threats in a dynamic way to represent each threat in different areas of the information system. This paper also supports the objectives of the research like identify the information security threats.

2.3.3.3 Remedies of Risks

There are many threats to e-learning, and here are some tools and methods that reduce the risk:

1) Access control using Firewall

A firewall is a blend of equipment and programming security system secured to avert unapproved access to a corporate system from outside the organization. Main principle is that all movement from inside to outside and the other way around must go through the firewall. To achieve this, all access to the local network must first be physically blocked, and access only via the firewall should be permitted. Only the traffic authorized as per the local security policy should be allowed to pass through. The firewall itself must be strong enough. One such firewall is shown in Figure 2.5.

2) Digital Right Management (DRM) on E-Learning Assets

One of the real procedures to be executed to lessen dangers connected with e-learning resources is computerized right administration. Shareable resource is the basic asset, for example, a static HTML page or a PDF report, or accumulation of documents, for example, pictures and a template. Advanced Right Management (DRM) makes the system more secure for its substance. E-Learning system is working either in a spread framework or in Internet where various rights joined with learner, educators content suppliers, chiefs thus on getting the most vital component as substance and organizations(Barik & Karfoma, 2012).

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

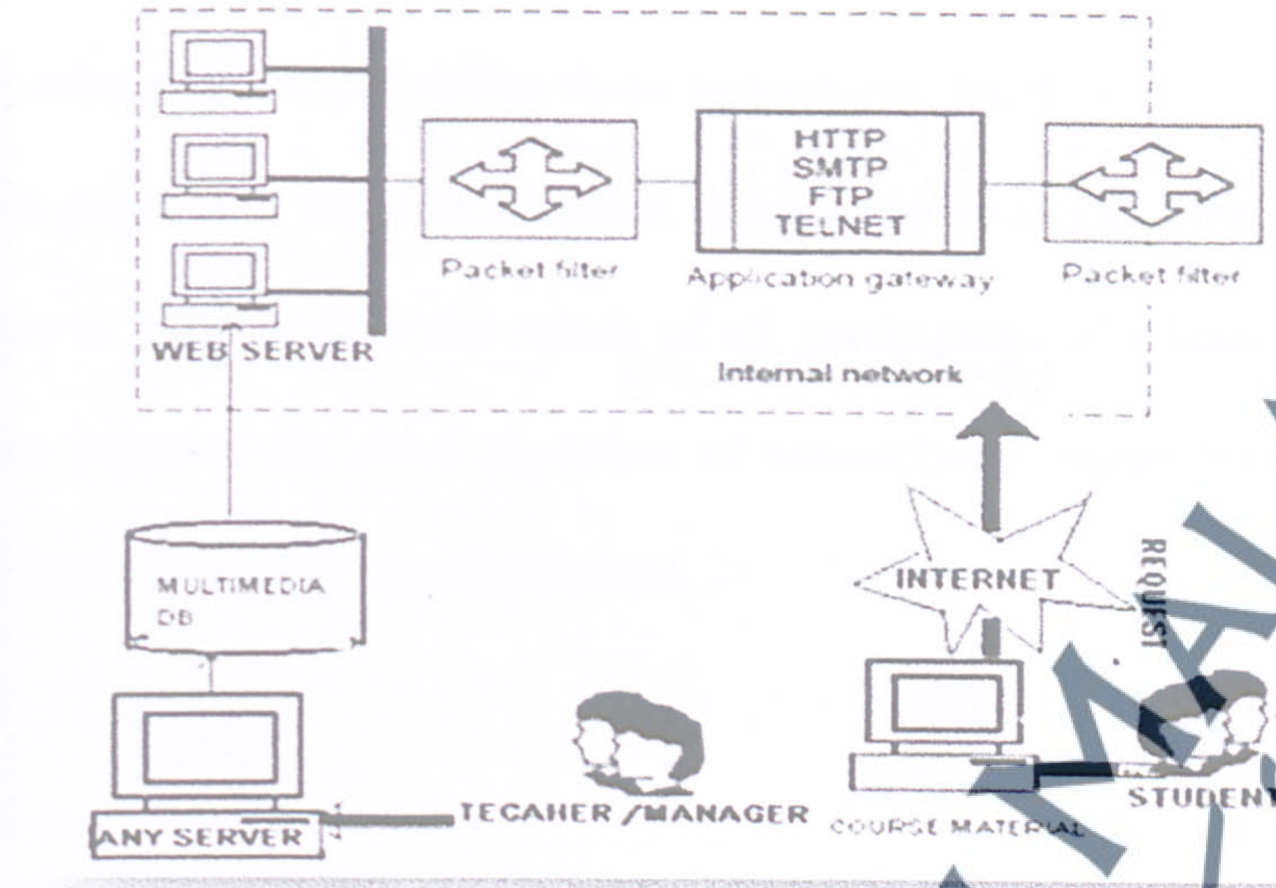

Figure 2.5: Organization of Secure (Source: Barik & Karforma, 2012)

3) Cryptography

The purpose of confidentiality is to ensure that information and data are not disclosed to any unauthorized person or entity. Also readers must able to rely on the correctness of the course. One of the techniques in this aspect is cryptography. Diverse cryptographic devices and strategies are required for the usage of security in Internet based exchanges. There are two sorts of calculations in cryptography (Barik & Karforma, 2012).

4) Secret-key algorithms

In secret-key algorithms the encryption & decoding key is the same, it requires the sender and receiver to agree on the key prior to the correspondence, the primary capacity of this calculation is encryption of information. Cases of such calculations are

Data Encryption Standard (DES), International Data Encryption Algorithms (IDEA), and Advanced Encryption Standard (AES).So just for encryption systems for E-Learning substance we can utilize these procedures. Barik and Karforma (2012), the aim of this paper is to focus on different risks called e-risks and their remedies called e-remedies to build trust in the minds of all participants of e-learning system, This paper also supports the third objective of researcher's research,that is to propose remedies for information security threats.

5) Public-key algorithms

Public key cryptosystems utilize one key (the public key) to encode messages or information, and a second key (the secret key) to decode those messages or information. Here three scientific models are fundamentally utilized Integer factorization, discrete logarithms and elliptic bend. Diverse open key calculations are RSA, El-Gamal, Diffie Hellman. We can utilize these strategies at the time of sending inquiry paper and accepting answer sheets. To authenticate a participant we can use following technologies using public key algorithm:

- Digital signature,
- Digital certificate

Gupta & Kuriachan (2013), the of this paper is to focus on different risks and hazards and of course remedies called e-solutions to build trust in the minds of all participants in the e-learning system. This article supports the third objective from researcher's research (Gupta & Kuriachan, 2013).

6) Neural Cryptography

It is a new approach based on Artificial Neural Networks (ANN) for information security in electronic correspondence. It is by and by a cryptosystem, which is in view of natural thoughts including the system building design, organic operations and the learning methodology. So the unpredictability of the era of the secured channel is direct with the span of the system. This natural system may be utilized to develop a productive encryption framework utilizing keys which change forever. It is exceptionally straightforward and quick to actualize in connection of conceivable assault at the time of exchanging e-learning archive. Volna et al. (2012), in this paper deals with using neural network in cryptography, e.g. designing such neural network that would be practically used in the area of cryptography. This article supports the third objective of researcher's research.

7) Elliptic Curve Cryptography (ECC)

As huge amount of textual and non-textual messages have to be transfer among participants so ECC will be stronger alternative than whatever other cryptography procedures. It is tried a mainstream key size require for RSA is 2,048 bits where ECC requires 224 bits for same security. Additionally both confidentiality and authentication may be saved if there should be an occurrence of e-learning record exchange utilizing elliptic bend advanced mark calculation (ECDSA). Gupta & Kuriachan (2013), in this piece of research work, emphasis is put on different risks and hazards and of course remedies called e-solutions to build trust in the minds of all participants in the e-learning system. This paper also supports the third objective of researcher's research.

8) Biometric Authentication

Among all authentication techniques like passwords, smart card, digital signature and advanced endorsement, there is no ensure that untrustworthy students will keep their watchword mystery.

Secret word may be abused at the time of accommodation of task, getting inquiry papers, downloading of course materials and others, where biometric authenticity would give better security (Lim & Jin, 2006).

9) Digital Watermarking

This procedure permits a single person to include add hidden copyright notices, sound, feature, picture signals. So media database server of e-learning framework may be secured against unapproved use by the method for advanced watermarking. At the point when additionally e-learning data like inquiry papers imperative study materials, and so on will undetectable to the viewer , the possibilities of hacking will be nil or less. Barik & Karforma (2012), in this paper, emphasis is given on different risks called e-risks and their remedies called e-remedies to build trust in the minds of all participants of E-Learning system.

2.3.3.4 Types of Security Attacks for E-Learning

E-learning system is huge, dynamic with a mixed bag of clients and assets. The main three sorts of security assaults as indicated by a security study are: insider ill-uses of system access, viruses and laptop/mobile device theft. The emphasis leans back on vulnerabilities and dangers particular to e-realizing, all the parts of E-learning framework, for example, web administrations, server PC frameworks, customer PC

frameworks, database frameworks can be undermined. Possible vulnerabilities that may affect the security of the online teaching learning system are summarized as follows.

- DDOS (Distributed Denial of Service): the attacker tries to lock the server using a high-speed connection, it jams the network card, or blocks the legit traffic.
- Search-SPAM: similar to the DDOS attack, a hacker may submit a lot of "dummy" searches using our internal search engine, using two or three letter words with high frequency (such as "of","for","and","in" etc). The result pages being a lot, these searches consume the most CPU time, both by Apache web service, PHP page generator and the MySQL database server.
- Key loggers may be installed by students who can steal teachers' passwords and modify their own grades (Ben et al., 2012).

E-Learning system allow numerous clients or applications to download, transfer and trade circulated data. Correspondence issues between end-clients' PCs and e-learning site in these systems are essential, as the systems are characterized by broadly scattered components regarding system topology and physical geography. Moreover, the systems regularly permit numerous to-numerous correspondence which gives intense abilities and permits numerous systems hubs to have the same correspondence at any given time.

Alwi and Fan (2010), in this paper explains the situation and existing research relating to security in e-learning. Furthermore, information security management is suggested

to contribute to preparing a secured e-learning environment. This supports the objectives ofresearcher's research.

Dangers to data frameworks may affect secrecy, trustworthiness and/or accessibility of an asset. Threats may operate in several ways such as destruction (the advantage is not recoverable), modification (changing the representation of an asset), exposure (infringement of need-to-know), and foreswearing of administration dangers for data security are listed below.

1) Act of Human Error or Failure (accidents, employee mistakes).

2) Compromises to Intellectual Property (piracy, copyright infringement).

3) Deliberate Acts of Espionage or Trespass (unauthorized access and/or data collection).

4) Deliberate Acts of Information Extortion (blackmail of information disclosure).

5) Deliberate Acts of Sabotage or Vandalism (destruction of systems or information).

6) Deliberate Acts of Theft (illegal confiscation of equipment or information).

7) Deliberate Software Attacks (viruses, worms, macros, denial of service).

8) Forces of Nature (fire, flood, earthquake, lightning).

9) Quality of Service Deviations from Service Providers (power and WAN service issues).

10) Technical Hardware Failures or Errors (equipment failure).

11) Technical Software Failures or Errors (bugs, code problems, unknown loopholes).

12) Technological Obsolescence (antiquated or outdated technologies).

Tatar and Karabacak (2012) his paper addressed the hierarchy based asset valuation method, where it is intended to minimize the common mistakes that were done during Information Security Management Projects.This paper supports the second objective in researcher's research.

In an e-learning situation, the system allows learners and professors to access it from remote locations. Usually, professors can do the following actions:

1- Load course material onto course sites for learners to retrieve.
2- Store assignment marks on the course web site.
3- Store tests to be written directly on the course web site.

While students can:

1- Recover lectures and course material.
2- Submit assignments to the course site from where teachers recover and mark such assignments.
3- Access the course web site to retrieve their marks for assignments.
4- Write different types of tests directly on their work stations with results marked by the system and stored on a course database.
5- Access course web sites to get the results of tests.

From here we can identify a few potential data security risks, such as.

1- Course material may be adjusted by unauthorized people.
2- Bogus course material may be loaded on course web sites, or web sites may be defaced.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

3- Submitted assignments can be replicated from course sites by unauthorized parties.

4- Submitted assignments can be changed or erased by unauthorized parties.

5- Access to test papers may be gained, test contents can be changed, or the test can be deleted before the scheduled test date.

6- People may masquerade as students and write tests on behalf of such students.

7- Students may get unauthorized help during the writing of tests.

8- The destruction of course web sites and course databases containing marks.

9- Denial of service attempts against course web sites preventing authorized students from accessing the web site.

10- Logon information of professors and students can be intercepted and misused.

The Information security risks identified above could be grouped in three general security categories:

1. Unauthorized release of information,
2. Unauthorized modification of information,
3. Unauthorized denial of resource use should be addressed by ensuring that the e-learning information security countermeasures are in place.

Vasilescu et al. (2011) in this paper addressed presents possible information security risks regarding e-learning and ways to tackle e-learning security challenges by adopting proper measures in this respect. This paper supports the objectives and methodology of researcher's research.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA
YSIA

2.3.3.5 Risk analysis

Risk analysis is the procedure of characterizing and dissecting the risks to people, organizations and government agencies posed by potential natural and human-caused adverse events. In IT, a danger examination report can be utilized to adjust innovation related targets with an organization's business goals. A danger investigation report can be either quantitative or qualitative (Barik & Karforma, 2012).

Qualitative risk analysis: A risk where probabilities and consequences and determined purely qualitative.

Quantitative risk analysis: A risk analysis that provides numerical estimates for probabilities or consequences-sometimes a long with associated uncertainties.

2.3.3.6 Steps for Risk Assessment

This is an important stage for security risks treatment. There are four steps needed to be carried out or needed to perform risk assessment, which are itemized below;

1. In this step is to determine if the risk is intentional or unintentional. It is from Insider or Outside, Software, Hardware, Antivirus, Spy, Trojan, SQL and others. These risks are also classified in terms of whether or not they will provide the effect of fabrication, modification, interruption or interception to the information and also decide who might be harmed, or not and how.
2. Evaluate the risk and decide on precautions: In this step is to know the security vulnerabilities for application employed for the e-learning and the extent of damage resulting from this risk.

3. Record the findings and implement them: When the administrator know the type of risk and damage resulting from it, then it can take the appropriate decision against this threat or minimize damage.
4. Review the assessment and update if necessary: Review, then carry out an assessment and updates the system, and learn from mistakes or flaws in the previous system.

This paper by Rausand (2013) supports the methodology for researcher's research.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA
جامعة العلوم الإسلامية الماليزية
USIM