NTNU
Norwegian University of
Science and Technology

Security challenges for e-learning ecosystems

Nazmus Sakiba

Master in Information Systems
Submission date: July 2017
Supervisor: Guttorm Sindre, IDI

Norwegian University of Science and Technology
Department of Computer Science

Abstract

E-learning systems are used by almost every educational institution and the system is upgrading day-by-day (e.g. traditional monolithic e-learning system to modern e-learning ecosystem or cloud-based system). E-learning system provides a lot of benefits in the educational process, at the same time security is one of the important concern for e-learning systems. To prevent loss of user's data and to prevent from any kind of damage, a secured e-learning system is a must. Every system has some security issues and challenges. To ensure the security of such system existing security issues and problems are investigated. The study is interested to know stakeholder's view on the security of e-learning system as well as how the user of the system deals with the security problem. The e-learning system has faced a lot of security issues before, which has been solved now. This kind of experienced issues will be discussed in this study with current security issues. This study is also investigated the security benefits and increased threats of shifting from traditional monolithic system to modern e-learning ecosystem or cloud-based system. The study has used a combination of two research methodologies (i.e. survey and interview). To find out stakeholder's view on the security issues and challenges of existing e-learning system a survey is used as a method. To find out the increased threats and benefits of security of modern e-learning ecosystem the interview is used. The answer of the survey is collected from the global student and the interview is conducted among some technical stuff of Norwegian University of Science and Technology, as they are able to provide some inside knowledge about this subject. This study is one of the first that has tested the link between trust, privacy, and security in the e-learning context. The result suggested that perceived trust can lead the e-learning system to a new direction as the user willingly provide more information to the system. The result also shows that the chance of violation of confidentiality, integrity, and availability is higher in the asset - assignment. Thus more attention should be given to protect the assets. E-learning system has already experienced some security issues like phishing attacks, identity theft, unauthorized access etc. Still, the system has some other minor security issues and challenges. The shifting from traditional monolithic system to modern e-learning ecosystem has a lot of other benefits, yet does not provide security benefits. Rather, this shifting increases the security threats. This research shows the findings of the increased threats of shifting to modern e-learning ecosystem. The findings of this study have various implications for research as well as practice. This finding of security challenges and issues will help to improve the security of e-learning system.

Acknowledgements

This Master Thesis is the part of my degree at the Norwegian University of Science and Technology. My specialization is in the field of Information System, at the Department of Computer and Information Science (IDI), in the Faculty of Information Technology, Mathematics and Electrical Engineering (IME).

In the work with the thesis, my supervisor Guttorm Sindre assisted me and made my work possible. I would like to direct special thanks to my supervisor, for continuous feedback, guidance, discussion, and for providing me some participants for the interview from his network.

The findings in this report were made possible by the contribution of 76 anonymous participants for the survey and 3 participants for the interview, who were willing to talk openly about the challenges and their thoughts about the research topic from their experiences. I thank them for their time, contribution, and honesty.

Saving the most important for last, I thank my wonderful parents who have taught me the value of learning, hard work, and encouraged my curiosity. Their guidance and support for everything have given me a better start in life than anyone could have asked for. Finally, I thank Amin - my husband - who has been a wonderful support, encouraging me to keep going with my sickness of pregnancy, and helped proofread the thesis. With humor and intelligence, he has brought me joy beyond what I deserve.

July 2017, Trondheim **Nazmus Sakiba**

Contents

List of Figures

List of Tables

Glossary

CBT	Computer Based Training. 4
CIA	Confidentiality, Intigrity, and Availability. 94
CSCL	Computer-Supported Collaborative Learning. 5, 6
DoS	Denial of Service. 78
ELES	E-learning Ecosystem . iv, 10, 11
LCMS	Learning Content Management Systems. 5
LMS	Learning Management System. iv–vi, 1, 3, 5, 12, 22, 23, 25–29, 38, 40, 55–58, 60, 61, 79, 93
NTNU	Norwagian University of Science and Technology. 5, 22, 41, 44, 53, 55, 56, 61, 95
TEL	Technology-Enhanced Learning. 6

Chapter 1

Introduction

The purpose of this introduction chapter is to provide a short overview of this thesis as well as present the motivation, goal, and research area of this thesis.

Learning online or e-learning is one of the fastest-moving trends in higher education. The term e-learning refers electronic learning where the acquisition of learning is performed by the computer and Internet-based courseware and local or wide area network. For example, one major type of e-learning is so-called Learning Management System (LMS). It offers the functionality for the teaching staff to deliver various types of information to the students of a course, either as broadcast to all students (e.g., course info, timetables, readings, lecture slides, exercise, deadlines) or to individual students (e.g., feedback on delivered coursework). It also offers functionality for students to find the information, respond to exercises, ask questions to the teacher etc. Of course, an LMS is not strictly necessary to achieve this, a typical alternative could be that each course has a web page for pull information, and the teaching staff uses email for push type of information, and students may also deliver exercises for instance by email. However, in most of the situations, a good LMS will be less cumbersome than this type of combined system of the web page and email. Especially for the students, the LMS can provide a one stop source for everything regarding the course, while sorting through email (which will also contain lots of other messages) will be much more time to consume and more easily cause some info to be overlooked. The LMS can also give the students a good overview of deadlines through a calendar function. If all courses they are taking in the same term used in the same LMS, they may have a joint calendar for all their coursework deadlines without the extra effort of maintaining this calendar themselves. For the teaching staff, the LMS might provide a much better overview of what information has been made available for the students and not, how many students have yet delivered a certain task, etc., as well as pending vs. completing tasks of the staff in reviewing such deliveries.

Security issues and challenges involved in the e-learning system are the main concern of this research. The motivation behind the study is given in Section 1.1. The goal of this study is presented in Section 1.2. Section 1.3 presents the research questions for the study. Section 1.4 gives a brief description of different forms of e-learning solutions.

1.1 Motivation Behind the Project

Nowadays, electronic learning or e-learning system is a compulsory tool, used in almost every educational institutions. The system increases the productivity of educational institution and the quality of educational service and support processes. E-learning is performing learning activities electronically using the internet. The assets of e-learning system are learning resources, online assessments, forum, mail, and notice; which allows a user to communicate at any time, from any place.

Like all other web-based systems, e-learning system is also exposed to computer security threats. Collection and storage of personal information happen many times in web-based system, without concern of users. Therefore addressing privacy and security issues are necessary and all necessary steps should be taken to make sure the security of the information of e-learning system [1].

Five kinds of significant participants of the e-learning system are Student, Teacher, Author, Manager, and System developer. An intruder can change the authentic learning content, question papers, mark sheet, certificates etc., which are communicated from Author to Student or Manager to Student. Electronic-risks occur at the time of electronic transmission. Common threats of this kind of system are network penetration, virus, eavesdropping, non-availability of server, theft and unauthorized change of data.

Students are the main participants and they are concern about their privacy and security while using the system. Such as they do not want their result will be revealed to others. Sometimes they want to post their question anonymously in the forum. They want a reliable system which will not frustrate them, by affecting their study performance. Hence, views and needs of the students are very important to make sure that the system is successfully implemented. Computer security is one of the reasons for rejecting such a system. Confidentiality, integrity, and availability are the computer security property. Normally the user of such systems is worried to lose the privacy and confidentiality of the sensitive information provided by them (i.e the user). Moreover the failure of the availability of the system makes disappointed the user. In the e-learning system, users will feel more confident to use the system when there will be trust, security and privacy mechanism. Students perspective in security is important since they are experiencing the service of the system day after day, and they can give feedback about the condition of the system to improve the system [2]. The people who are involved in maintaining the e-learning system has also dealt with the security issues in their daily work. They could also give some deeper knowledge about the security issues and challenges involved in the e-learning system. Moreover, the e-learning system is changing from traditional monolithic system to modern e-learning ecosystem or cloud-based architecture. No doubt, this shifting facilitates the learning process and giving a lot of new opportunities to the teachers, students, as well as in administrative work. As, the focus of this study is on security, whether the shifting leads any security benefits as well as increased any security threats is also important to investigate. The result of the investigation could be used to improve the security of new generation e-learning system in future.

1.2 Goal

Security is a common issue for all web based systems. This study wants to find out what are the security issues the students are facing. Also, which security issues of e-learning system are at the high risk. Therefore, this study will present the student's view on the security challenges of the digital learning environment in different countries. A questionnaire is used to get the answer from the respondents who are mainly the university students from the different countries. The result of this study might help the developer to understand student's view as well as to update the e-learning system according to the need. Thus, the efficiency and quality of the e-learning system will be improved and the acceptance of this kind of e-learning system will be increased. By this way, the student will get more secure learning environment and service from the e-learning system.

Another goal of the study is to find out what are the increased security threats as well as what are the opportunity of improved threats we get by shifting from traditional monolithic learning system to current e-learning system. Only the increased security benefits and threats led by this shifting are focused on this research, though this shifting has other benefits. However, this study is not interested in the other opportunities led by this shifting. Knowing security benefits and problems are very important for this modern system. This study will help to know if there is any security risk reduced by this shifting which was involved in the traditional system, as well as about the increased threats. The identified increased threats from this study will be helpful for the system developer of the system. They will focus more on the identified part to cut the security risk of the modern e-learning ecosystem. By this way, the educational institution who are getting benefit from the modern e-learning ecosystem will be secured from all kind of attacks, and the customer will rely more upon this new system.

1.3 Research Question

The pre-work of this study has gathered what are the possible security threats exist in e-learning and what are the available solutions for the threats. Now the concerned area is the view of the major stakeholder (i.e student) of the system related to the security threats and the views of the technical staffs on the security benefits and problems of the shifting from traditional monolithic system to modern e-learning ecosystem.

- **RQ1: How do key stakeholders view the security challenges of digital learning environments?**

The first area of concern is to find out the key stakeholders' believe on how much secure do the digital learning system is. The second area of concern is to measuring security threats involved in the e-learning system on the basis of basic computer security properties - availability, integrity, and confidentiality. The third area of concern is to show the encountered security risks and the last area of concern is measuring the trust of the stakeholder towards the e-learning system by using the perceived trust, perceived security, and perceived privacy. The overall students' view on security enables us to know how much secured each Learning Management System (LMS) is, how the security of different LMS varies among countries, what kind of violation they have experienced, and how much harmful if some certain kind of violation occurs to the system.

- **RQ2: In what ways is the shift from traditional monolithic local systems to each university to systems with a modern ecosystem or cloud architecture, with possible sharing of resources across universities, seen as (a) an increased threat to security, and/or (b) an opportunity to improve security?**

This research question is the quite advanced question and the average stakeholders might not able to answer this part. For this part of this study, it is more natural to interview security experts to get inside knowledge on the subject. As the participants of this part are the responsible person of managing the e-learning system, The first area of concern will be asked about security issues and challenges involved in the system and to know their experience about it. The second area of concern is to know whether the e-exam reduce the tendency of cheating in the exam. The last and main area of concern is knowing about the shifting from monolithic system to a modern ecosystem or cloud architecture, as well as about the increased security threats and opportunities improved by this shifting.

1.4 The State of Art

E-learning is an ambiguous term which is used to describe a different kind of learning solution. Today's different kind of e-learning solution are [3]:

- Computer Based Training(CBT)
- Learning Management Systems (LMS)
- Learning Content Management Systems (LCMS)
- Computer-Supported Collaborative Learning (CSCL)
- Technology-Enhanced Learning (TEL)

Below an overview is given for these different kind of learning solutions:

1.4.1 Computer Based Training(CBT)

CBT can be described as a form of interactive and pedagogical course solutions where a software product installed on a personal or networked computer [4]. They are normally designed as short step-wise courses with a mix of text, pictures, video, and exercises presented to the user. The examples of suppliers of such CBT solutions are RosettaStone.com (provides DVD-courses to learn languages) and IndustrialLogic.com (provides on-line courses for programmers).

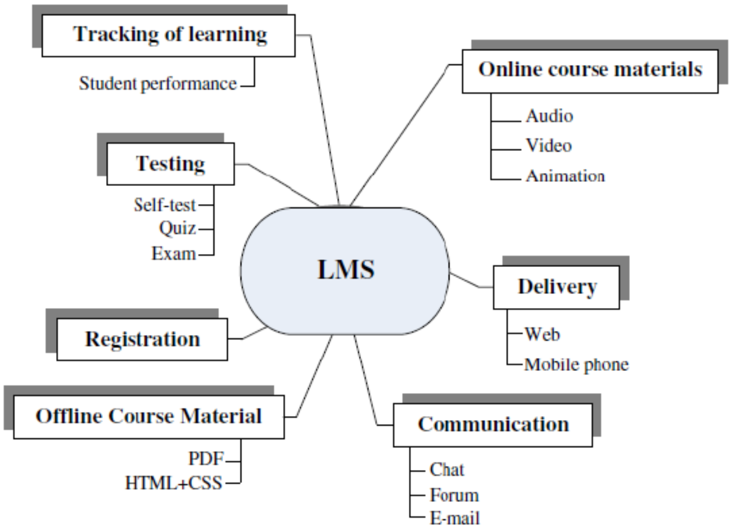


Figure 1.1: Structure of the Learning Management System (exact figure from [6])

1.4.2 Learning Management Systems (LMS)

LMS are administrative supporting tools which automate tracking, and reporting of students in the educational institution all over the world [5].

They give the opportunity to centralize and automate administration, self-service and self-guided service, support portability, and standards, to distribute and reuse content to the course and ease digital hand-in of assignment. The example of LMS are Moodle, Blackboard, It's learning, Canvas, Desire to Learn etc. The largest LMS of Norway are It's Learning and fronter. Though from this year, NTNU started to use Blackboard instead of It's Learning. On the other hand, the LMS 'Desire to Learn' is largely used in USA and Canada.

1.4.3 Learning Content Management Systems (LCMS)

LCMS is an application which allows a method for managing content or lessons from a central location. It enables large-scale of re-usability of content. Authorized user can edit, add, view content with the lower level of access. Therefore, LCMS is a further development of the LMS specialized in content the management of e-learning content. LCMS also allows indexing and powerful search in digital content. SumTotal.com and OutStart.com are the suppliers of LCMS. 'Atutor' is an example of LCMS [3].

In Figure. 1.2 Admin is managing LMS i.e managing training, distributing courses over Internet, on-line collaboration, student self-service. On the other hand, Authors and Tutors are managing content or lesson by creating, storing, and reusing.

1.4.4 Computer-Supported Collaborative Learning (CSCL)

CSCL is a growing type of E-Learning that provides a solution by giving users a tool that let them collaborate and share content [3]. The examples of fully integrated CSCL solutions are "Knowledge Practices Environment (KPE)" [7]. It uses a digital work surface named "shared space", that lets users switch between working together

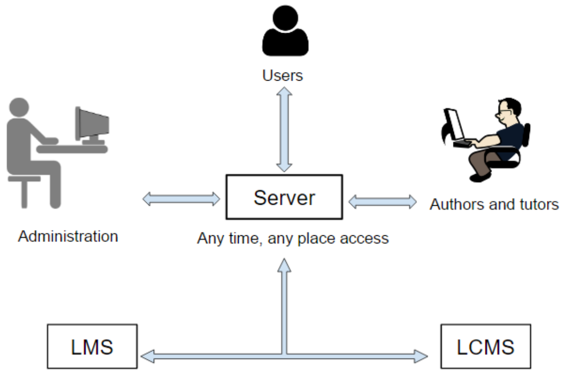


Figure 1.2: LMS and LCMS

and individually with the same content. Outside of such solutions, CSCL mainly has combinations of Wiki's, Blog's and existing LMS's which are experimented with by pioneering teachers (According to Kane, 2010). Some partly considered solutions under the CSCL umbrella are, Online communities and each Smartboard. A lot of Online Communities ("social network services") have tools that make sharing of content simple. SmartBoards are interactive blackboards which can be used in classrooms and allow them for multiple user interactions.

1.4.5 Technology Enhanced Learning (TEL)

TEL is a software that is being used to make mind maps, or electronic spreadsheets to support or enhance the learning process [8]. It could refer to video-conferencing tools used in remote education like Maratech used at NTNU; IT-technology that teachers use in correlation with teachings like SmartBoards or so-called Mindtools. A challenge with the TEL-tools is that they are often too complex, and therefore draw time and the cognitive capacity away from the content of the education. BYOD (Bring Your Own Device) emerges another significant development in TEL, where students use their own device (i.e smartphone) to support their learning [9]. Facebook is another example which can enable easy networking among the students and the location of people with similar study interest.

1.5 Outline of the Research

The rest of the thesis is organized as follows.

Chapter 2 describes the background theory of this research. This chapter starts with a brief description of the e-learning software with its functionality. Then a short explanation of the term 'e-learning ecosystem' and 'cloud-based e-learning system'. Then it represents the responsibility of each stakeholder as well as the security requirement of each asset of the e-learning system. The final section of this chapter is on security in e-learning system, which starts with a brief description of IT security, the principle of security, and some common security threats and measures. It also explains the necessity of security in the e-learning system.

Chapter 3 discusses the detailed research methodology of this study. This discussion includes the process of collecting the answer of the research question. This chapter also includes participant recruitment, questionnaire design, setup, and testing of both survey and interview, as well as post work of the collected answer from the both methods.

Chapter 4 describes the result of this research. This chapter starts with the participants' demographics, and then it shows the satisfaction on the security of e-learning system among the participants. Then the findings on stakeholder's view on the security of the e-learning system describe. The findings on the security issues which are already experienced and which currently exist are discussed there. This chapter also shows the findings on the security opportunities and increased threats of the shifting from local monolithic system to e-learning ecosystem or cloud-based system.

Chapter 5 presents the concluding remarks of the thesis and discuss some recommendation for the further investigation.

Chapter 2

Background Theory

This chapter represents the background theory of the research including the topic which will be used all over the study.

2.1 e-Learning Software

To design, manage, and run the educational process in the educational institution several commercially available tools are used, they are known as e-learning software. This e-learning platform allows the user to log-in to the system securely using the browser. In most cases, this kind of software includes a database-centered syllabus with links to internal or external web pages, time-monitored testing, discussion groups, and email. It allows manager and administrator to track course completions, current status, or performance of employees. In fact, all employee activities can be tracked. This tracking information could be used for performance evaluation, competency management, and other related functions. Some popular e-learning packages are: Blackboard, Lotus Learning system, etc.

The main purpose of this kind of e-learning software is to enhance the learning process (i.e. improve classroom teaching, learning methodology, and company records). This kind of platform is not only deliver the learning content, but also handles registering courses, course administration, skill gap analysis, tracking, and reporting, etc [10].

2.1.1 Functions of the e-Learning Software

This e-learning platform allows the manager and administrator to perform several important functions in an organization. The following are some of the function which proves to be invaluable to the administrator and the manager of the system [11].

Making a Course Calendar This feature enables the users to view the available training programs or courses at one glance. As a result, the learner can send requests for registrations to those course or training program that they are interested in easily.

Tracking and Reporting This kind of feature provides a wide range of standard and custom summaries and detailed reports, which helps the learner to view his average test scores, final test scores, single user report, company log-in record, the summary of overall tests taken, etc.

Administration This helps to administrative work for example, it facilitate the ways and means of getting enrollment approval, individual, batch registration, and verifying prerequisites etc.

With this kind of functionality, e-learning system provides all possible facilities to enhance the learning process. It has the ability to engage and motivate training which increases the success rate of students. The educational process is going on by using the technology which makes it an interesting and exciting way of learning. Moreover, it simplified the learning process as well as reduced the time and cost. It also provides the interactive learning environment and anytime, anywhere learning which also makes the learning system more efficient.

2.2 e-Learning Ecosystem (ELES)

e-Learning ecosystem is a solution of business issues and a way to improve organization's ability.

Chang and Guetl elaborately described e-learning ecosystem (ELES) by using the two terms biotic and abiotic constituents from the biological ecosystem. According to the Encyclopedia Britannica, an ecosystem is a "complex of living organisms, their physical environment, and all their interrelationships in a particular unit of space" [12]. The abiotic or non-living constituents of the system are addressed by the physical environment of the system, on the other hand, living or biotic constituents are consists of all its living members.

In ELES biotic component are formed by learning stakeholders. The learner's learning strategies, styles, and preferences, their competency level plus many other attributes can be considered in this biotic component. The abiotic components are closely linked with the biotic component in a symbolic relationship. The abiotic components include the use of dynamic learning utilities and media; by linking with the learning community's attributes and the response from the teaching and learning group. Specific learning content management system (LCMS), learning management system (LMS), content delivery system (CDS), and other learning utilities may be used. The interactions and relationships between the biotic and abiotic components are also influenced by internal and external environmental conditions.

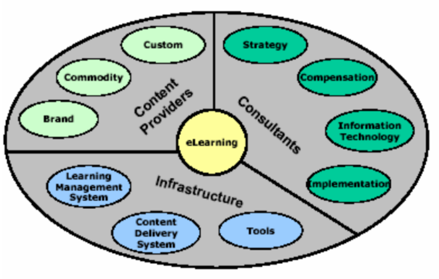


Figure 2.1: ELES component (exact figure from [13] page: 2)

Learners can contribute to the internal influences in the form of interaction and collaboration, as the learning patterns are controlled by them. External conditions like the evolution and the innovation of the application system and the technology; other cultural and sociological aspects may lead to a change in the use of the application and technology. External e-learning ecosystems may interact and impact the internal system. It must be realized that a disconnection to a component may be detrimental to the success of the e-learning ecosystem. It is required that all components of ELES must integrate and work harmoniously and there must be a balance in the utilization

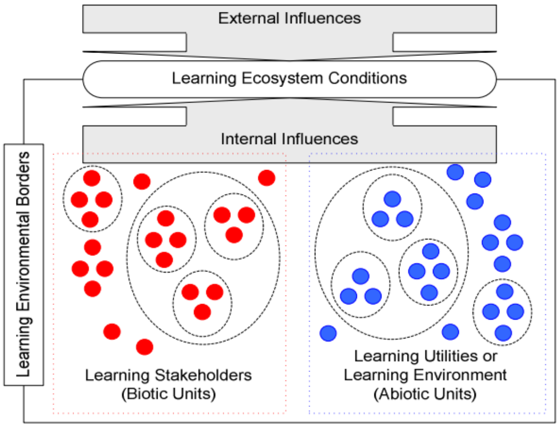


Figure 2.2: Representation of the ELES (exact figure from [14] page: 2)

of each component [15]. Brodo represents a Figure 2.1 where he describes all the components of ELES to implement e-learning solution. On the figure, the components are divided into three groups: content providers, consultants, and infrastructure. Chang and Guetl [15] represents a simplified e-learning ecosystem in Figure 2.2 which has four elements (1) as biotic unit there is 'learning communities and other stakeholders' (i.e. instructor, content provider, pedagogical experts, and instructor designers etc.) (2) as abiotic units there is the learning utilities (i.e. the learning media, technologies, and tools applied in traditional teaching methods), (3) Learning environmental borders (4) Learning ecosystem condition with external and internal influences.

2.3 Cloud-based Learning System

Cloud-based e-learning ecosystem allows a reliable, flexible, cost-efficient, self-regulated, and QoS-guaranteed infrastructure. The contributions of cloud system in e-learning ecosystem are as follows [16]:

1. Cloud based e-learning ecosystem provides the infrastructure which is QoS-guaranteed. For example time, cost, reliability, and hardware performance (i.e. CPU bandwidth and memory size, and sustains SLA-oriented resource allocation) [17].

2. It also provides the support of various application, as well as making the system rapid, and convenient to get the required computation, and storage.

3. Cloud provides real-time configuration information, and resource utilization information. It also allocates resources on demand, and improve the usage rate of resources.

4. The cost is cut down through the automatic resource management, which helps to solve emergencies rapidly, as well as to achieve labor-intensive jobs.

Cloud-based e-learning system provides a low-cost solution to the researchers, faculty, and students of an educational institutions. The browser-based application provides the additional benefits of accessing through mobile devices as well as a variety desktop computers and laptops. One of the most important feature of cloud system is scalability, and the key technology which makes it possible is virtualization.

2.4 Stakeholders and Their Responsibilities

The success of e-learning system depends on the extent to which is satisfies the needs and addresses the concerns of its key stakeholders. The stakeholders of the system are students, instructors, educational institutions, content providers, technology provider, accreditation body, employers, provider, etc. Stakeholder to stakeholder responsibilities according to Wagner are as follows [18].

Students Students are the targeted stakeholders of e-learning system. The entire electronic learning system makes the student more independent than the traditional system.

Student to student responsibilities in the system is: participate in collaborative exercises to enhance learning, and share experiences. *Student to instructor responsibilities is:* participate proactively in exercises and provide feedback regarding overall effectiveness. *Student to institution responsibility is:* to use the e-learning technologies according to institutional policies. *Student to content provider responsibility is:* provide feedback regarding the appropriateness of content for e-learning. *Student to technology provider responsibility is:* provide feedback regarding the effectiveness of technologies. *Student to Accreditation body responsibilities is:* Demand accreditation for e-learning programs, and Provide feedback.

Instructors E-learning system like LMS deals with the administrative challenges, which are used to relieve the teacher of this administrative work so that the teacher can spend more time on the purely pedagogical challenges. Other types of function to deal with the pedagogical challenges are, for instance, sharing of content among teachers, the more effective overview of student knowledge during the course, etc. The e-learning system allows the instructor to upload files and information to the system and take online classes.

Instructor to student responsibilities is: provide effectively designed courses incorporating e-learning content and provide technical, and motivational support to encourage use. *Instructor to instructor responsibilities is:* share experiences and encourage use and promote standardization. *Instructor to institution responsibility is:* use e-learning technologies according to institutional policies and standards. *Instructor to content provider responsibilities is:* ensure the protection of copyrights and provide feedback regarding the level of effectiveness experienced by students collectively. *Instructor to technology provider responsibility is:* to provide feedback regarding the effectiveness of technologies. *Instructor to employee responsibility is:* to educate on the validity of e-learning.

Educational Institutions Educational institutions are the main stakeholder of this system. They adopt e-learning system to allow a lot of student in their institution. An important consideration for the institution is how effective the system is for the institution.

Institute to student responsibilities is: standardize the e-learning experience across courses, provide technical support, and protect sensitive student information. *Institution to instructor responsibilities is:* provide training in instructional design and technology, provide technical support, provide incentives, and enforce standardization. *Institute to content provider responsibilities is:* ensure the protection of copyrights and provide funding for content development. *Institute to technology provider responsibilities is:* provide feedback to improve future versions and supply appropriate infrastructure to support technology. *Institute to accreditation body responsibilities is:* adhere to accreditation standards, and provide evidence for quality assurance. *Institution to employee responsibilities is:* seek course accreditation to provide evidence for quality assurance and educate on the validity of e-learning.

Content providers Content is either provided by the instructor or from the outside source. The main concern of content provider is their intellectual capital rights.

The content provider (CP) to student responsibilities is: to select appropriate content and media for e-learning and comply with usability standards. *CP to instructor responsibilities is:* to provide content that meets course and program needs and comply with learning and usability standards. *CP to institution responsibilities is:* to provide content that meets institutional needs and comply with learning standards.

Technology provider They are motivated to provide technical support in order to run the learning system efficiently.

Technical Provider (TP) to student responsibilities is: consider learning principles when designing, allow adjustments for individual learning styles, and comply with usability standards. *TP to instructor responsibilities is:* consider usability and teaching principles when designing and comply with learning and usability standards. *TP to the institution and content provider responsibilities is:* comply with standards for interoperability, and provide technical support and training. *TP to TP responsibilities is:* comply with existing standards, and collaborate to develop new standards when necessary. *TP to employee responsibility is:* to provide an effective learning environment to maximize the learning of potential employees.

Accreditation bodies By the growing demand of e-learning, it is important for the accreditation body to encompass e-learning by their standards.

Accreditation body (AB) to student responsibility is: to enforce standards to ensure the quality of accredited courses. *Accreditation body's responsibility to all other assets (i.e. instructor, institution, content provider, technology provider) is:* to clear guidelines for requirements and timely services. *AB to employee responsibility is:* to enforce effective standards to ensure the quality of graduates.

Employers Employers of the learning ecosystem are one of the stakeholders. *Employee to Student responsibility is:* to recognizes the validity of e-learning. *Employee's responsibility to the assets like the instructor, Institute, and TP responsibility is:* to provide feedback regarding the success of graduates. *Employee to content provider responsibility is:* to provide feedback regarding relevance in the workplace. *Employee to accreditation body responsibility is:* to ensure that standards provide appropriate measures.

In this research, targeted stakeholders are students and employers of the educational institution. As they are handling the system they might experienced some security issues or they might have some feedback on security of the e-learning system.

2.5 e-Learning Assets with Security Requirement

Klobucar et. al. defined e-learning assets as e-Learning content (Exam, Notes, Grade), Cryptographic key content, User personal data, Messages between users, Different group membership data, Network bandwidth, Message integrity and Message availability [19]. This study considers the assets like Learning content, e-Exam, Student result, User profile, Forum content, Assignment, Announcement. Brief description of the assets are given below [20]

Learning resources or content The learning resource or content are assets that provide the student for example lecture notes to help in studies. The contents are mainly live classroom, curriculum, lectures, notes, assignment discussion, planning and schedule, previous exam question, certificate, receipt of semester fee, book, related paper or article etc. Learning content should be available and should not be changed original content while downloading. Distributed notes should not be changed by an unauthorized person and the lecture notes should have copyrights. To avoid damage to the reputation of the department, all information should be error free.

Online assessment or e-exam This asset involved with exam question and answer sheet of the student which should be protected. The exam question will reveal to the student only in the exam hall, and it should not be available before the exam. The system has to be protected from any action to crash the system to ensure the availability of the examination. Privacy, integrity, availability, confidentiality, and non-repudiation of the assessment are major factors that influence the success of the on-line assessment. Non-repudiation is important to know that actual student is taking the exam and submitting the answer sheet. The system should only allow registered student as well as it should be able to detect cheating in the e-exam.

Students' results or records Student results are also managed by the system. This asset includes the results of the continuous assessment, assignment, and exam result. Some security requirement of this assets are – the result information should be known by owner only and the information can only be accessed by the student and facilitator. Unauthorized modification of the result data will cause loss of integrity and privacy. Wrong inputting (i.e. human error while typing) of students' marks will also effect of the integrity of students' mark.

User profile or user account User of e-learning system are the student, instructor, faculty member, etc. For instance, a student profile contains his identities such as his name, address, student id, etc.; his demographic profile such as age, gender, race, language, etc.; his learning profile such as qualification, interest, etc.; course history and current courses [21]. The user profile can be managed by the administrator. The user can update their own profile. The information should be protected to safeguard the privacy of users. The accuracy of profile information is also important otherwise, it will affect adversely.

Forum content This service is used by students and facilitators for the discussions. Students can send questions and await responses from other students or facilitators. In the forum, students send questions if they have doubt about anything and await responses from other students or facilitators. Some of the discussion probably involves a sensitive issue. Thus, the privacy of this forum must be protected. Students would not publish controversial problems if their identity could be revealed. Each message sent to this forum should be tracked through the log files to prevent repudiation among users.

Assignment This asset shows assignment details including submission date, assignment type, marking criteria, etc. When submission date has passed it does not allow the student to submit the assignment. Administrator and facilitator use this service. The information is not really sensitive since wrong information does not really affect the system and there is still space to make amendments.

Students submit their assignment by uploading their work into the system. After verifying the assignment, student got the result of their assignment. Students submit their assignment by uploading their work into the system. The assignment should not be modified or tempered when facilitator receives it. The e-learning system has to maintain the availability of the system especially when the due date is near. The student will feel frustrated if they cannot submit their assignment within due time because of the unavailability of the system. The submitted assignments need to be proven to avoid repudiation.

2.6 Security in e-Learning

This section will describe security, the principle of the information security, the threats involved in the e-learning system and their protection mechanism, and why security is needed in the e-learning system.

2.6.1 IT Security

IT security or cyber security is the degree of resistance to, or protect from harm, which applies to the computing device (i.e. any device with a processor and some memory), as well as the computer network (i.e. public and private network, including the whole internet). This field includes hardware, software, data, procedures, and people, by which digital system (i.e. equipment, information, and service) are protected from unauthorized access [22].

Software security is the software engineering to make the software function correctly under malicious attack [23]. Application security is a part of software security, as it is the protection of software after the software is already built.

This study focuses the application security as the e-learning system is already developed. After developing the e-learning system there might have some security problems which the stakeholders are facing, the back-end employees might deal with some security problems every day while they are facilitating the e-learning system for the students and teachers. This study will identify the security problems involved in the system in order to avoid any kind of attacks or damages of the e-learning system. These identified problems could also be mitigated later by the mentioned procedure like penetration testing, and different types of coding to prevent the system from threats and risks.

2.6.2 Principles of Security

Confidentiality, integrity, and availability (i.e. CIA triad) are the heart of information security. These are interchangeably referred to the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics, and basic building blocks etc. Violation of CIA is analyzed in this study to understand the security of the e-learning system. There is another methodology for identifying threats developed by Microsoft. The acronym of STRIDE is Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege. Among the six threats tampering is the violation of integrity, information disclosure is the violation of confidentiality, and denial of service is the violation of availability. These threats are analyzed to understand the security of the e-learning system.

2.6.3 Involved Threats and Protection Mechanism

The threats come in many different forms among them, some common threats are software attacks (e.g. viruses, worms, phishing attacks, etc.), theft of intellectual property, identity theft (i.e. an attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information), theft of equipment or information, and sabotage (i.e. the destruction of a website in an attempt to cause loss of confidence on the part of its customers) [22]. Threats to confidentiality are malware, intruders, insecure networks, social engineering, and poorly administered systems. Cryptography and access control are the two main mechanisms of protection of confidentiality. The protection mechanisms of integrity are grouped into two types: detective mechanisms, which are intended to detect unauthorized modifications when preventive mechanisms have failed, and preventive mechanisms, such as access controls that prevent unauthorized modification of information. The principle of least privilege, separation, and rotation of duties are some control that protects integrity. The attack against availability is known as DoS (Denial of Service) attack. Natural and man-maid disaster affect the availability of a system. Disaster recovery planning (i.e. regular and reliable backups) is intended to minimize losses [24].

2.7 The Need of Security in e-Learning System

Learning system on the internet is not only offering a lot of facilities for increasing efficiency and reducing cost but also offering unlimited potential risks and threats. The internet provides greater access to data, which makes the system more vulnerable to data theft. Moreover, the increasing use of standard protocols and interfaces has provided major advantages for the user community. Nevertheless, this facilitates the initial access for an attacker too. The use of the virtually standard database, spreadsheets, and other software applications, as well as standard hardware processor together with continuing evolution and dissemination of hacking tools, and techniques, makes the attacker's subsequent deeper intrusion into the e-learning system more easier. Such attacks are difficult to detect and trace to their source. The hacker can work from a location which is safer from legal retribution, thus making such attacks ever more attractive [25]. Thus it is important to maintain security in e-learning system to protect the system from destruction. It is also important to investigate current security problems and take action to measure it to get an efficient e-learning system. Moreover, the e-learning system is developing day by day, which brings a lot of opportunities to the education system as well as it increases security risks too. Thus, to get this advanced opportunity in an efficient way a secure educational system is a must.

2.8 Conclusion

This chapter presents the background study of this thesis. A brief description of the term e-learning system with its functionality is given first. The term e-learning ecosystem and cloud-based learning are used in research question 2. This two term are described shortly. Different responsibilities of stakeholders are explained. This chapter also gives an explanation of security requirement of different assets. The focus of this thesis is security, therefore some theory of information security and principles, some common threats, risk management process of e-learning system are described. The necessity of security in e-learning system is also pointed out in this chapter.

Chapter 3

Research Methods

This chapter describes the methodology used in this research, the reasoning of choosing the methods, and the strength and weakness of them. In addition, this chapter has also presented the design, setup, deployment process of the questionnaire and interview guide.

Figure 3.1 shows the overview of the process of this research. The first activity is to define the research questions for the research.

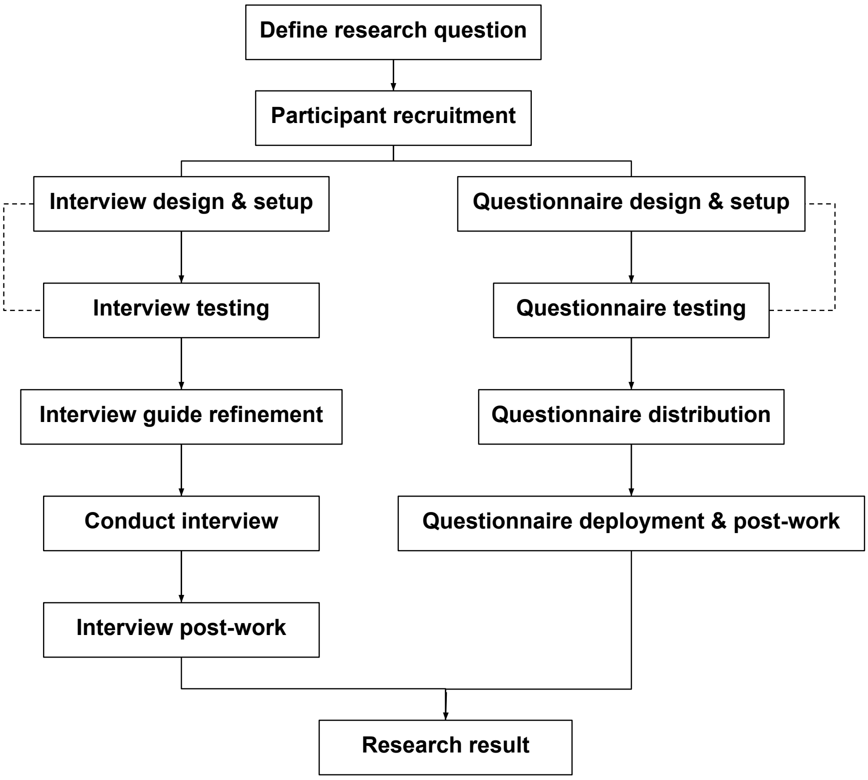


Figure 3.1: The research process

The next activity was the recruitment of participants. A plan has made on the process of participant recruitment. Then, the design and setup of the questionnaire and interview guide started in parallel. Different types of questions are structured for questionnaire and interview. Questionnaire of the survey is made for the general student, who may not have enough knowledge in the security of learning management system. On the other hand, the interview questions are structured for the technical person. After design and setup, both the interview and survey questionnaire went through testing. The result of this test has been used in an iteration process to make improvements of the questions. The testing also gives an idea that from which area this study will get more participant, which type of stakeholder will respond more in the survey. The questionnaire of the survey has been deployed as well as the interview guide was refined, and then interviews were conducted after the testing was completed. When the answers have been received, the results are analyzed.

3.1 Research Question and Research Methodology

Defining research question was one of the first activity of the research process. Two research questions are decided for this research. One is *"How do key stakeholders view the security challenges of digital learning environments?"* Another research question is *"In what ways is the shift from traditional monolithic local systems to a modern ecosystem or cloud architecture, with possible sharing of resources across universities, seen as (a) an increased threat to security, and/or (b) an opportunity to improve security?"*

After deciding the focus of the research, research methods are needed to seek the answer to the research questions, appropriate research strategies. There are several methods for real world research. People could be *watched* and could be tried to work out what is going on. People could be *asked* about it. According to research language, this watching is called *observation*, and asking is called *interviewing*, using *questionnaires*, and administering *tests*. The interview is usually taken place face to face and in person. Questionnaire and test may be presented without direct, personal interaction. The simple rules of thumb for selecting a method is [26]:

- *Observation* is used to find out what people do in public.
- *Interview* is used to find out what people do in private.
- *Interview, questionnaire, attitude scale* are used to find out what people think, believe, feel.
- *Standardized tests* are used to determine their abilities or measure their intelligence or abilities.

For this research, security of e-learning tools could be investigated in various ways, from purely technical approaches (i.e. security testing, automated analysis of source code to find vulnerabilities), through a combination of technical and soft approaches, towards using soft approaches only (i.e. questionnaire, interview). Technical approaches might be better at showing what security (or vulnerability) e-learning software actually has, while an approach with questionnaire and interviews would rather reveal people's perception of this security. The tech approaches have some disadvantages like they are time-consuming and possibly difficult to perform for the system which is proprietary (i.e. source code not available). Hence one would easily end up having to investigate the security of one product rather than a broader look at the field in general. On the other hand, relying on human information rather than a technical approach (e.g. interview, questionnaire) had the advantage of being able to consider several systems with less work effort. The disadvantages are that the informant's knowledge about the security might be inaccurate. Comparing questionnaire and interviews, questionnaires have the advantage of being able to collect information from a large number of informants quite cheaply, and results are easy to compare and analyze. The gathered information might be somewhat shallow. On the other hand, interviews can give deeper information on *how* and *why* type of questions. However, interview is more time-consuming method and harder to analyze. Fewer people can be used as informants. Though there are several advantages and disadvantages in all the methods, a mixed method with the combination of *questionnaire* and *interview* is selected from the nature of the research question which is discussed below briefly.

The first research question is ***How do key stakeholders view the security challenges of digital learning environments?***

The nature of the question is that it needs broad coverage and response from many people. Such research question is fit for the research methods like *questionnaire*. In this research, the key stakeholders are students. The questionnaire is adapted to collect information from any kind of human population, and it is useful to collect data from the global student. The questionnaire provides a simple and straightforward approach to study attitude, values, beliefs, and motives on a particular subject. It has a high amount of data standardization too. The questionnaire will be structured in a way which will help to find out students security experience, feedback on security issues, and their belief in the system. Despite this, the collected data are affected by the characteristics (i.e. memory, knowledge, experience, motivation, and personality) of the respondents. The respondent may not necessarily report accurately their beliefs, attitudes etc. [26].

The second research question is ***In what ways is the shift from traditional monolithic systems local to each university to systems with a modern ecosystem or cloud architecture, with possible sharing of resources across universities, seen as (a) an increased threat to security, and/or (b) an opportunity to improve security?***

It is a more complicated question which only the experts would be able to answer reliably. The *face-to-face interview* is the right method for this research question, where interviewee will share their deep thoughts about the subject. While there is no chance to clarify the question in the survey, in the face-to-face interview it is possible to clarify the question, if the respondent face any problem to understand the question. Moreover, the presence of interviewer in this type of interview encourages participation and their involvement. Nevertheless the data may be affected by the characteristics of the interviewer and unwittingly the interviewer may influence the responses of the informant. The data may be affected by interactions of the interviewer or the respondent characteristics. The respondents may feel their answer are not anonymous and become less open while answering [26].

3.2 Participant Recruitment

As described above the answer of the research question is obtained from the key stakeholder of the system as well as security expert of the system. The participant of this research are the student who are the main stakeholder of the e-learning system and the technical provider.

It was pre-planned that the survey question will be tested among different stakeholders and different countries to get an idea about, from which kind of stakeholders and countries this study may get more response. In the testing phase, it is noticed that it is easy to get the response from the student as they are huge in number in any educational institution comparing other stakeholders. Moreover, they are the targeted stakeholder for any e-learning system. It is also easy to spread the survey among the students, for instance, the survey can be shared more than one class-mates or friends of a student. Thus, global students are the main participants of the survey.

The questionnaire is sent to the participants of different countries. The author can manage to get more response from the countries where the author has the connection. The countries are Norway, USA, Canada, Malaysia and Bangladesh. The people from authors network from these different countries can spread the survey to their friends, family, and classmates or colleges of the university. In the testing phase of the questionnaire, it is found that all of the stakeholders are the student as the people of authors network are the student. It is also noticed that the participation rate of Malaysia is very low and it seems difficult to spread the survey there. It is decided that the response from Malaysia will be included in this study only when the data will analyze among different continental. From the wider distribution to all of the countries Norway, USA, Canada, Malaysia and Bangladesh are selected for this study. These countries are from different parts of the world, and they are culturally very different. This choice of countries maybe more globally representative than the countries who have similar kind of culture, for instance, a survey covering Norway, Sweden, Denmark etc. Therefore, the global participant of this research are mostly from Norway, USA, Canada, and Bangladesh.

Using both direct email and Facebook message, the survey invitations sent to the participants. The ideal number of participants has been set at somewhere between 15 to 20 for each country. In total, 76 participants are identified for questionnaire through this recruitment techniques.

For the interview part, Prof. Guttorm Sindre helped to find out one relevant person who's responsibility is to manage the functionality of Blackboard in NTNU. After the interview, this person has suggested two more relevant people for this study who are also responsible for managing the LMS. Therefore, in total three people are found for the interview.

3.3 Questionnaire

As described above the answer of research question 1 (RQ1) is obtained from the method *questionnaire* and the answer of research question 2 (RQ2) is obtained from the research method *interview.* Different kind of questions is structured for this two methods. Hence, there will be no chance to get similar kind of answer from the two methods.

General kind of security questions are made for the students, keeping in mind that they may not have much knowledge about the security. As they are the main stakeholders of the system, they are interacting the system most of the time comparing to the other stakeholder. They have better opinion about the views on the security issues of the e-learning system. On the other hand, technical stuff are the participant of interview part. As they can provide some deeper knowledge for the study. Thus, the pattern and wording of question of this two methods are varies depending on the participants. Simple words are used for the student as they might not have deeper knowledge about the security of the system and relatively technical term is used in the question of interview, as the participants are technical stuff.

The results of the questionnaire will mainly be used to start a discussion on the relevant topic. These discussions are the foundation for the finding of the study.

3.3.1 Questionnaire Design

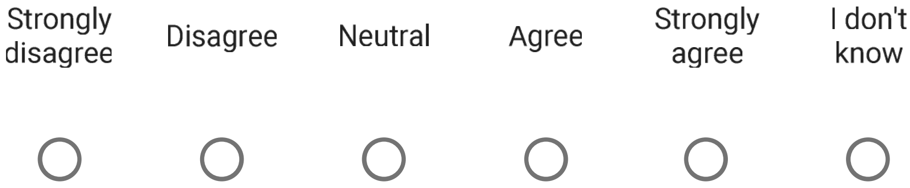
There are many choices and factors can be taken into account, for developing a questionnaire. Following literature presents the factors and the choice of designing the questionnaire.

Medium of the survey There are two types of questionnaire; one is paper based survey which can be sent to the participant by mail, another one is electronic survey conducted over the internet. As the participants are recruited globally, processing of paper survey and sending them out will be excessive amount of work or a high cost. The advantages of the electronic survey is that it can automatically calculate averages, return comparisons, and supports complex skip patterns. Online survey is chosen for this study, and Google Form [27] is used as a tool which helps to make an online survey. Making survey, and calculating the results of the survey are easy in Google Form. It has a lot of option to share or send the survey to the participants.

Wording of questions It takes time to decide the exact wording of the questions and alternatives in the questionnaire. The survey has to made using proper wording before sending the survey. Because after sending the questionnaire, there would be no opportunity to make clarification or alter the survey. After making the survey, the wording were tested and corrected before sending it to the participant. The technical terms which are used in security like spoofing, tampering etc., are avoided, because the participant may not familiar with this kind of technical terms. Hence, this type of technical words are modified into simple words which might be understandable by all the student. More complex part of questionnaire was broken down into several simpler questions. On the testing phase, it was noticed that some participants are confused about the term ‘e-learning’ or ‘LMS’. The problem is solved by giving a brief description with the example, showing in Figure 3.4.

Length of the survey A long length survey could be a reason of discouragement to take part in the survey. The expected length of the survey is found to give a negative correlation between the number of participants starting the survey, and the number completing it [28]. To get more relevant information there was a reason to ask more questions, perhaps including some deeper questions that requires the respondent to think a lot. On the other hand, this research wants as many people as possible to complete the survey, which is a reason to ask fewer and simpler question. For this reason, the decision is the part of a difficult trade-off. One of the important goal of the survey is limiting the size of the survey, to make sure that there would be no unnecessary loss of participants. Based on these, a goal of ten minutes has been set for the completion time of the questionnaire. Therefore, after preparing the survey with the necessary and important questions, the questionnaire has tested to estimate how many time is required to complete the survey. The estimated time is almost ten minutes.

Likert scales There are several questions asked in the survey, which required the respondents to answer on a scale. Because this kind of likert scale used to represent respondent's attitude towards the subject. In this survey, the points of scale varies according to the necessity of the question. 3 point likert scale is used to measure the likelihood of risk on each assets, and 4 point likert scale is used to measure the harmfulness of risk, showing in Figure 3.12 and 3.13. 5 point likert scale (excluding the option I don't know) are also used, illustrated in Figure 3.2.

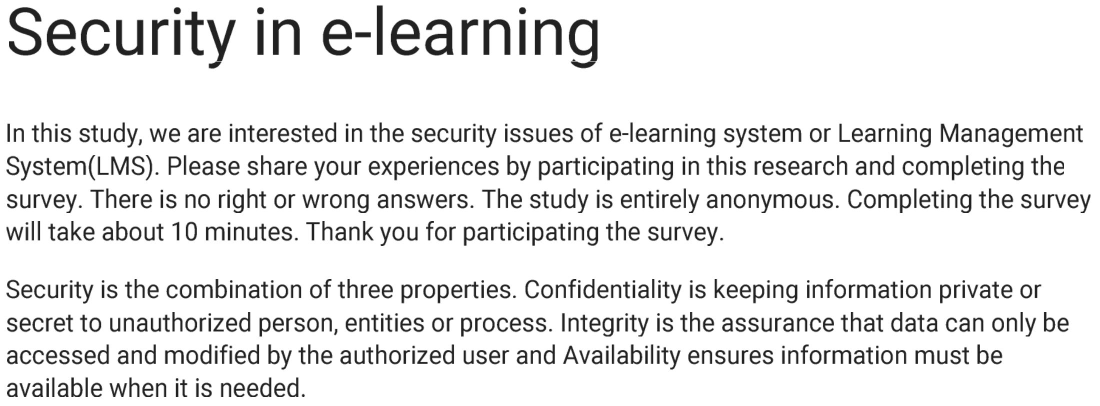


Strongly disagree	Disagree	Neutral	Agree	Strongly agree	I don't know
○	○	○	○	○	○

Figure 3.2: The six point likert scale used in the survey

It was desirable to keep the option *Neutral* (i.e. having an option with equal distance to each extreme), while not giving too many granular options. Another option *I don't know* is kept in almost each question. Because, participants may get confused or do not understand which option to choose from the points in a question. Without this option the respondent may feel force to answer a question which they might not have any idea.

Anonymity People can give true answer if they find the survey is anonymous. Only sincere and honest answers are beneficial for any kind of research. Most of the time people do not like to give their personal information in the survey. Moreover, the un-anonymous survey discourages people to take part in the survey. At the beginning of the survey design process, the questionnaire required some personal information like name, email address etc. Having the respondents name and email could potentially useful, if there was a wish to contact some of the respondents for clarification of their answer (esp. in free text boxes), or if some of them seemed to have a lot of relevant knowledge and thus be candidates for interview. However, collecting this kind of personally identifiable information make the survey much more sensitive, and maybe causing a need to apply to an ethical committee/ NSD for permission before the data collection start. This process may cause too much delay to complete the study. Moreover, it is important to get sincere and honest answer from the participants. Therefore, personal information part has dropped from the questionnaire. While inviting the people to take part into the survey, it has been written that the survey is anonymous. It is also written in the introductory page of the survey with other security information, shown in Figure 3.3.



Security in e-learning

In this study, we are interested in the security issues of e-learning system or Learning Management System(LMS). Please share your experiences by participating in this research and completing the survey. There is no right or wrong answers. The study is entirely anonymous. Completing the survey will take about 10 minutes. Thank you for participating the survey.

Security is the combination of three properties. Confidentiality is keeping information private or secret to unauthorized person, entities or process. Integrity is the assurance that data can only be accessed and modified by the authorized user and Availability ensures information must be available when it is needed.

Figure 3.3: The landing page of the survey

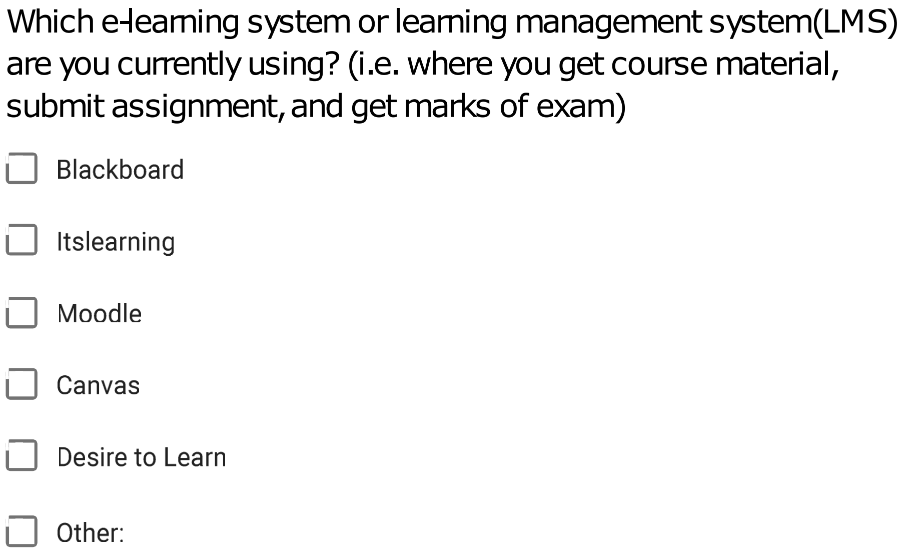
Question order The introductory part of the questionnaire begins with some description of the survey and security (showing in Figure 3.3), then it has some general type of questions which are kept to understand what type of LMS user the participants are, which LMS they are using etc., which may help to analyze the result from different dimension. Second part is about basic security questions, the questions of third part is about the encountered security risk, and then the closing part is kept for feedback.

The introductory part of the survey will help the respondent, get to know that the survey are interested in the security challenges and issues of the e-learning system or LMS. Then the general question will help them to understand that this study wants to know about their e-learning experience on security issues. The question of basic security components can give the respondent better understanding about what kind of security issues we are interested in. This order can help the respondent to understand the topic step by step, so that they can answer knowingly what they are answering.

3.3.2 Questionnaire Setup

This section will describe the setup of the questionnaire. The questionnaire, which is distributed among the respondent are showing in Appendix A. The first part of the questionnaire is about a general information of survey, and the participants are asked to give the general information about the LMS, they are using.

Introduction In the introduction part of the survey, showing in Figure 3.3, interested research areas are mentioned. It provides the information that the survey has no right or wrong answer, and it is anonymous. It also gives an idea about the estimated time to complete the survey. It gives some more information about the basic part of security. This information let the informant know that the survey is based on the security challenges of their e-learning system. This general information about the survey is important to share with the participants to let them know what this survey wants from the participants. Without this general information, the participant will be clueless while answering and the participants may leave the survey in the mid-way.



Which e-learning system or learning management system(LMS) are you currently using? (i.e. where you get course material, submit assignment, and get marks of exam)

□ Blackboard

□ Itslearning

□ Moodle

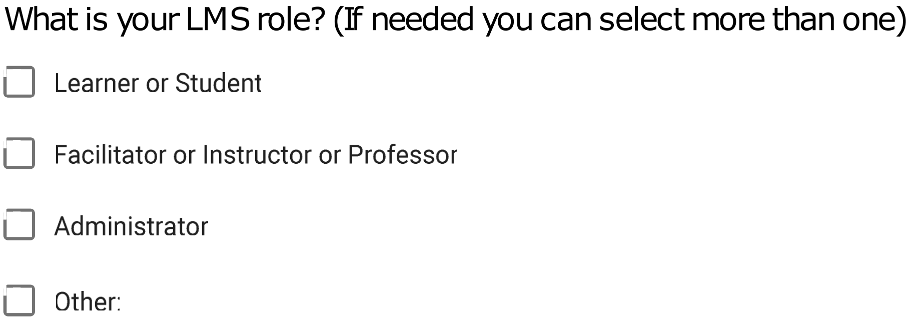
□ Canvas

□ Desire to Learn

□ Other:

Figure 3.4: Question 1: Define user of an LMS

Figure 3.4 shows the first question of the survey, asking the participants about the name of LMS, they are using. This general question helps to analyze the data LMS-wise. Therefore, the weakness or strength of different LMS, can be recognized. How many people are using a certain LMS, and which country is using which LMS, can be known from this question.



What is your LMS role? (If needed you can select more than one)

□ Learner or Student

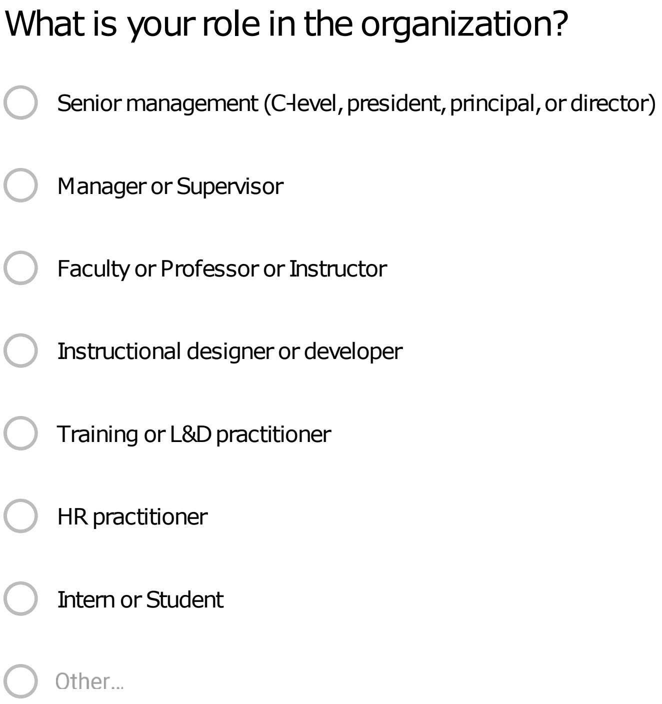
□ Facilitator or Instructor or Professor

□ Administrator

□ Other:

Figure 3.5: Question 2: LMS role

The second question of the survey is showing in Figure 3.5, which wants to know the LMS role of the respondents. Though the main respondents of this survey are the students, some students may have part-time job in the university. This kind of participants can select more than one option and can write his responsibility in the university. As some student has some other job in the university then he might have different kind of LMS role. Because of this, he might use more time in the LMS, comparing to other student.



What is your role in the organization?

○ Senior management (C-level, president, principal, or director)

○ Manager or Supervisor

○ Faculty or Professor or Instructor

○ Instructional designer or developer

○ Training or L&D practitioner

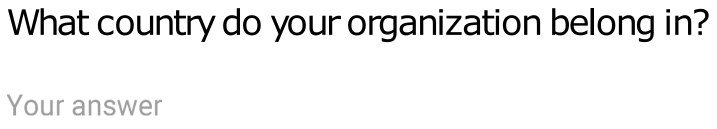
○ HR practitioner

○ Intern or Student

○ Other...

Figure 3.6: Question 3: Position in the organization.

Figure 3.6 shows the next question of the survey, which is about the working role of the respondents in the institution. As our main participant in this survey are students, this question will make sure whether the participant is student or not, as well as what is his additional duties in the university.

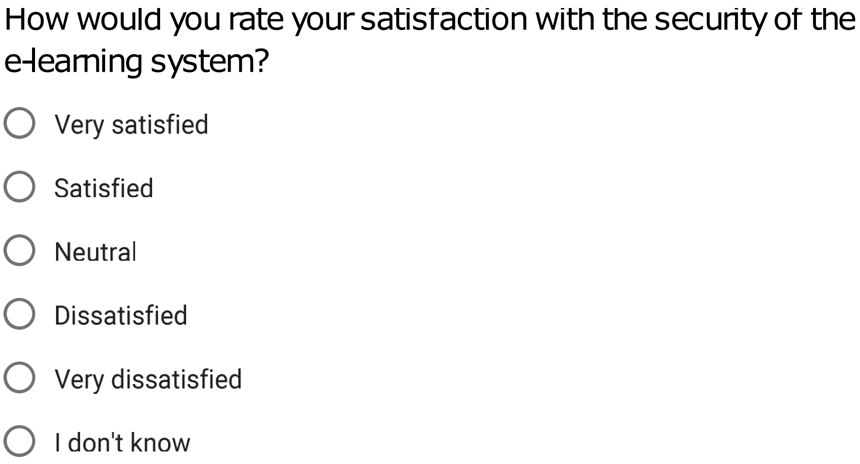


What country do your organization belong in?

Your answer

Figure 3.7: Question 4: Name of the country of the organization.

The 4th question wants to know about the name of the country showing in the Figure 3.7, where the respondent are studying. This question will let to know the respondents are studying in which country, and the LMS are using from which country. As the survey is made for global participants, it is important to know from which part of the world the respondent is studying.



How would you rate your satisfaction with the security of the e-learning system?

○ Very satisfied

○ Satisfied

○ Neutral

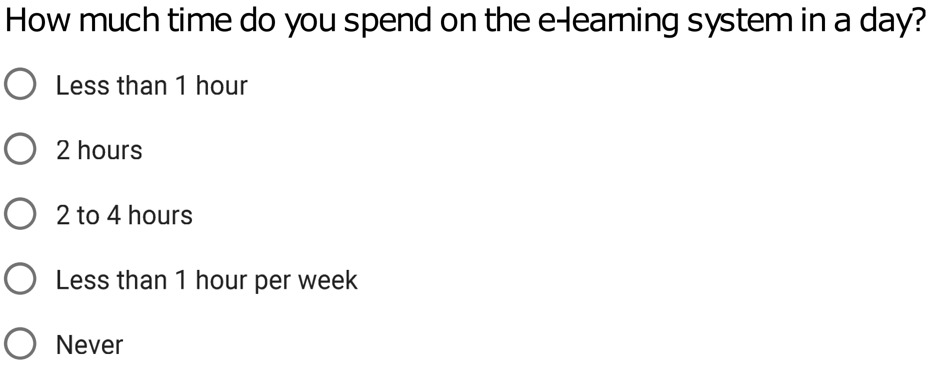
○ Dissatisfied

○ Very dissatisfied

○ I don't know

Figure 3.8: Question 5: Satisfaction rate.

The question 5 is used for calculating satisfaction rate showing in Figure 3.8. That means, how satisfied the respondent is with the security of the e-learning system or LMS. This question will also help to analyze the result from a different angle like, comparing the answer of satisfied respondent and dissatisfied respondent etc.



How much time do you spend on the e-learning system in a day?

○ Less than 1 hour

○ 2 hours

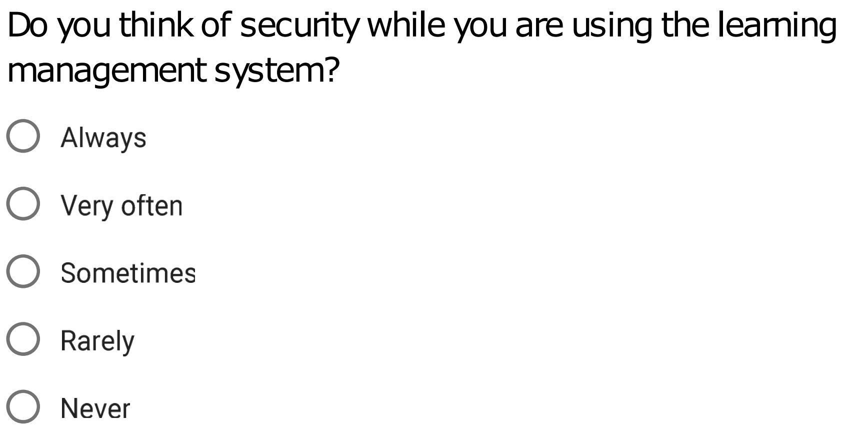
○ 2 to 4 hours

○ Less than 1 hour per week

○ Never

Figure 3.9: Question 6: LMS using time.

The 6th question wants to know how much time a user spend on the e-learning system in a day. This question also helps to know what kind of user the respondent is, how much time of a day he/ she spend in the LMS. If he spend less time or do not use the system at all than he may not have enough experience with the e-learning system.



Do you think of security while you are using the learning management system?

○ Always

○ Very often

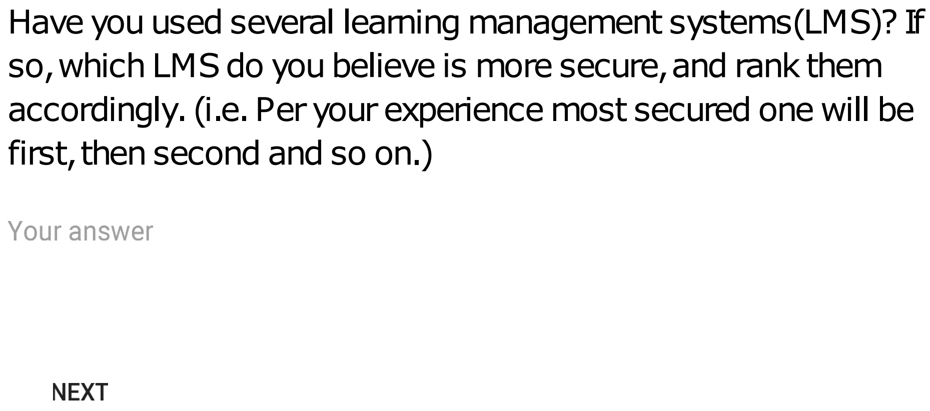
○ Sometimes

○ Rarely

○ Never

Figure 3.10: Question 7: Security awareness.

7th question is about security awareness, showing in Figure 3.10. To analyze how much the respondents are aware of the security issues, when they are using the system.



Have you used several learning management systems(LMS)? If so, which LMS do you believe is more secure, and rank them accordingly. (i.e. Per your experience most secured one will be first, then second and so on.)

Your answer

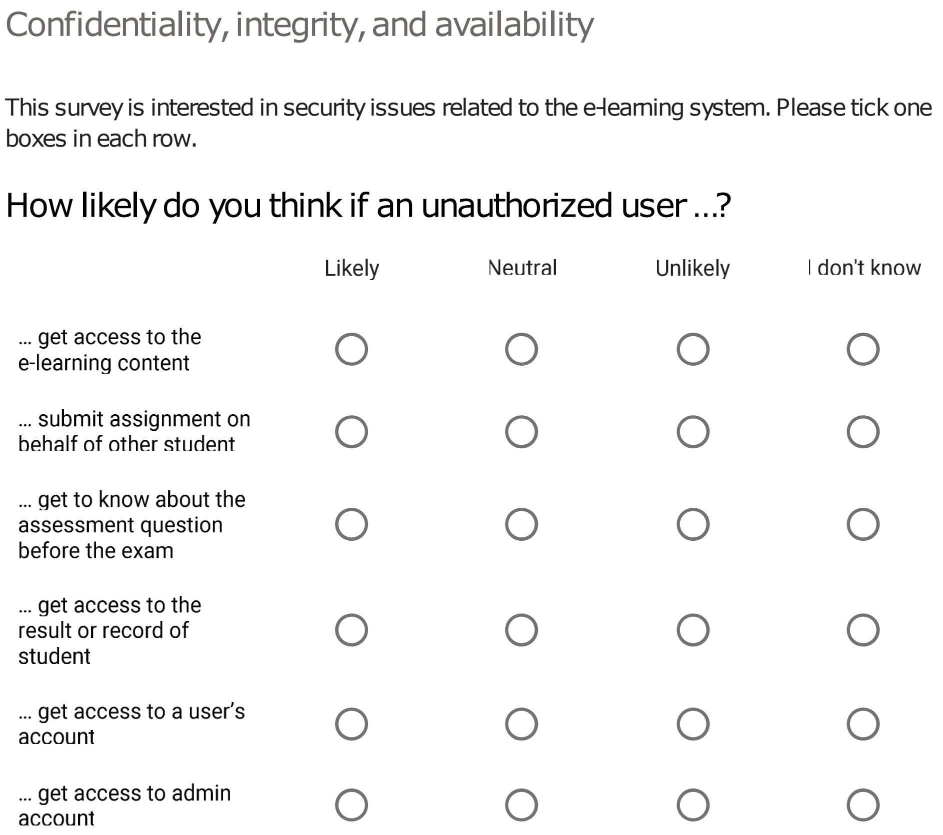
NEXT

Figure 3.11: Question 8: Ranking of LMS on the basis of security.

There are many users who have experience of more than one LMS. This kind of user can compare which LMS is better than other, on the basis of the security. Question 8 is for that kind of user, showing in Figure 3.11. Therefore, this question is not for all, and it is not a mandatory to answer.

This introductory part consists of 8 questions. The answer of these question will give an idea about the type of LMS user and give some feedback about the LMS.

Basic security risk measurement As described in the introductory text of the survey that security has three properties, they are Confidentiality, Integrity, and Availability. These three properties will be used to measure, how much secure the system is to protect the assets of the system. The risk on each assets are measured by likelihood and harmfulness. Because of that, the questions on the property confidentiality and integrity are structured almost with the same statements as well as same likert scale. In case of availability different statement and likert scale are used for the same assets.



Confidentiality, integrity, and availability

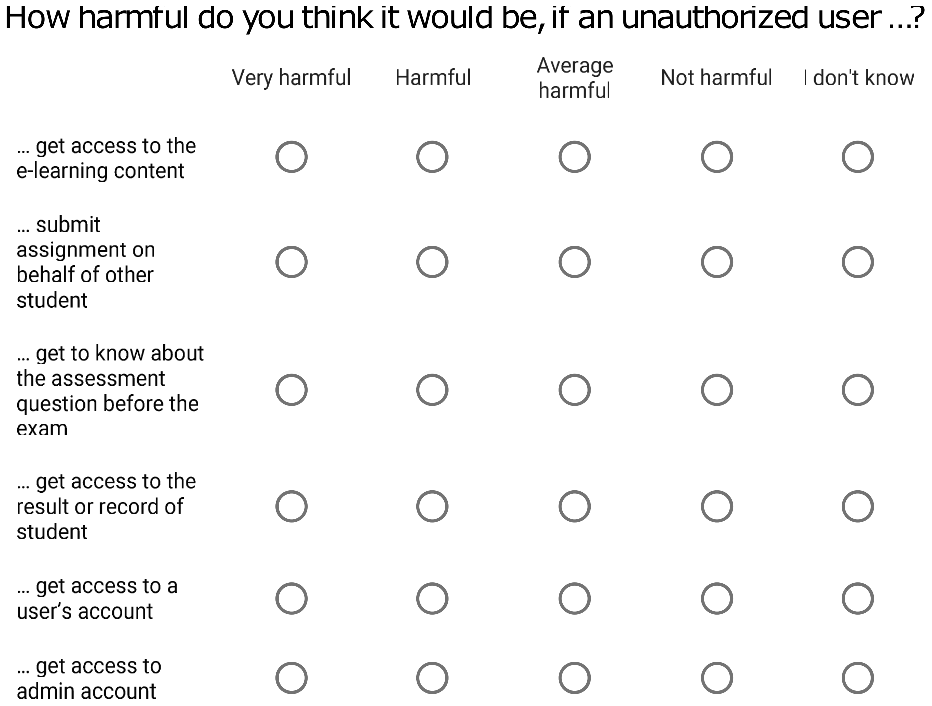
This survey is interested in security issues related to the e-learning system. Please tick one boxes in each row.

How likely do you think if an unauthorized user …?

	Likely	Neutral	Unlikely	I don't know
… get access to the e-learning content	○	○	○	○
… submit assignment on behalf of other student	○	○	○	○
… get to know about the assessment question before the exam	○	○	○	○
… get access to the result or record of student	○	○	○	○
… get access to a user's account	○	○	○	○
… get access to admin account	○	○	○	○

Figure 3.12: Question 9: Respondents perspective on the violation of confidentiality on the basis of likelihood

Figure 3.12 shows the question 9 which is used to measure the possible risk of the assets like e-learning content, assignment, assessment question, student record, user's account, admin account, and personal information. This question has six statements and the statements are answered on a 3 point likert scale, which are Likely, Neutral, Unlikely. 'I don't know' is also used, so that the confused respondent who really do not know what to answer, may choose this. This question helps to understand participants believe on the possibility of occurring each type of violation on *confidentiality* stated in each statement.

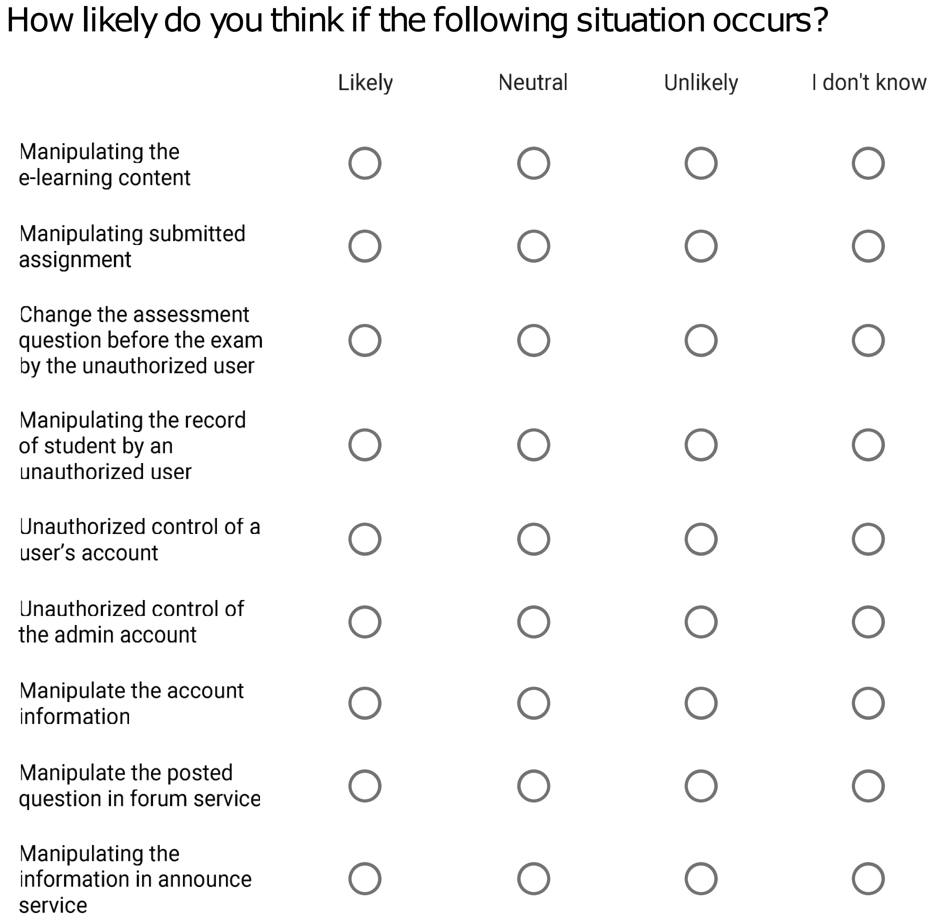


How harmful do you think it would be, if an unauthorized user ...?

	Very harmful	Harmful	Average harmful	Not harmful	I don't know
... get access to the e-learning content	○	○	○	○	○
... submit assignment on behalf of other student	○	○	○	○	○
... get to know about the assessment question before the exam	○	○	○	○	○
... get access to the result or record of student	○	○	○	○	○
... get access to a user's account	○	○	○	○	○
... get access to admin account	○	○	○	○	○

Figure 3.13: Question 10: Respondents perspective on the violation of confidentiality on the basis of harmfulness

The 10th question of the survey is showing in Figure 3.13. The answer of that question will help to measure how much harmful it is, if any of the mentioned risk happened on the assets of the e-learning system. The same six statement of previous question are used here and the question has four point likert scale, they are Very harmful, Harmful, Average harmful, Not harmful. Another option I don't know is also given for the confused respondents. This question help to understand how much harmful the situation will be if stated violation of *confidentiality* will happen to the system.

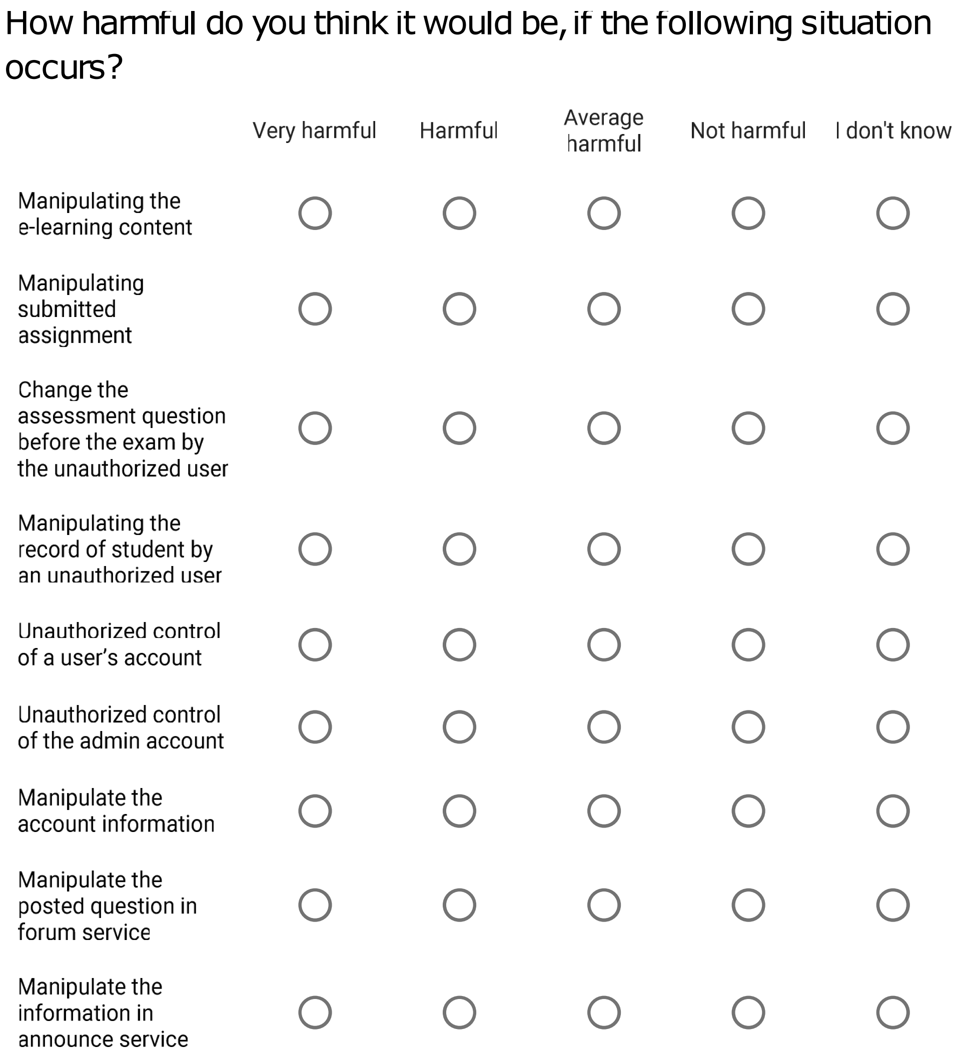


How likely do you think if the following situation occurs?

	Likely	Neutral	Unlikely	I don't know
Manipulating the e-learning content	○	○	○	○
Manipulating submitted assignment	○	○	○	○
Change the assessment question before the exam by the unauthorized user	○	○	○	○
Manipulating the record of student by an unauthorized user	○	○	○	○
Unauthorized control of a user's account	○	○	○	○
Unauthorized control of the admin account	○	○	○	○
Manipulate the account information	○	○	○	○
Manipulate the posted question in forum service	○	○	○	○
Manipulating the information in announce service	○	○	○	○

Figure 3.14: Question 11: Respondents perspective on the violation of integrity on the basis of likelihood

The 11th question of the survey is showing in Figure 3.14. This question will measure the possibility of the violation in *integrity* for each mentioned statement. This question designed with nine statements, and has three point likert scale same as question 9 of Figure 3.12.

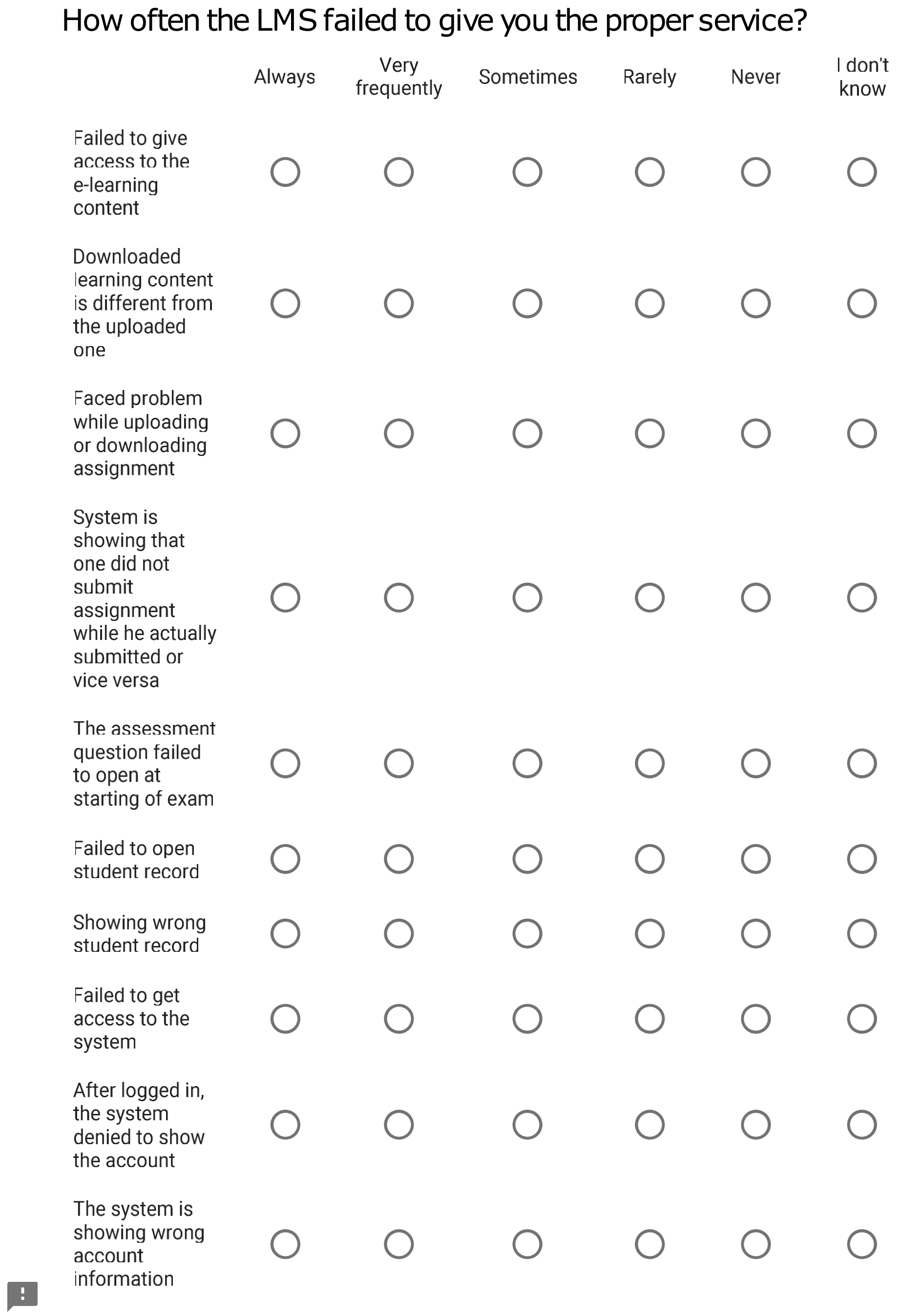


How harmful do you think it would be, if the following situation occurs?

	Very harmful	Harmful	Average harmful	Not harmful	I don't know
Manipulating the e-learning content	○	○	○	○	○
Manipulating submitted assignment	○	○	○	○	○
Change the assessment question before the exam by the unauthorized user	○	○	○	○	○
Manipulating the record of student by an unauthorized user	○	○	○	○	○
Unauthorized control of a user's account	○	○	○	○	○
Unauthorized control of the admin account	○	○	○	○	○
Manipulate the account information	○	○	○	○	○
Manipulate the posted question in forum service	○	○	○	○	○
Manipulate the information in announce service	○	○	○	○	○

Figure 3.15: Question 12: Respondents perspective on the violation of integrity on the basis of harmfulness

The 12th question of the survey is showing in Figure 3.15, which has almost the same statement as question 11. However, the likert scale is different, like the harmfulness of the violation of confidentiality of question 10 Figure 3.13. This question will measure how much harmful the system will be if mentioned violation in *integrity* of each statement will happen.



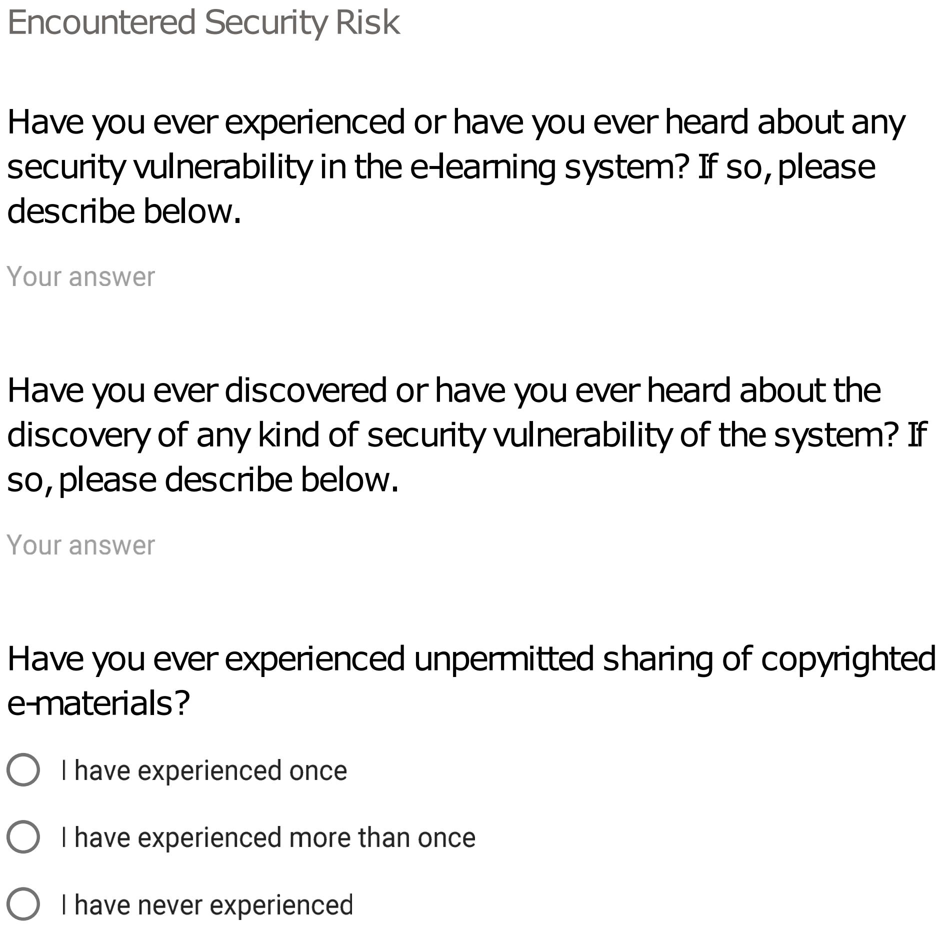
How often the LMS failed to give you the proper service?

	Always	Very frequently	Sometimes	Rarely	Never	I don't know
Failed to give access to the e-learning content	○	○	○	○	○	○
Downloaded learning content is different from the uploaded one	○	○	○	○	○	○
Faced problem while uploading or downloading assignment	○	○	○	○	○	○
System is showing that one did not submit assignment while he actually submitted or vice versa	○	○	○	○	○	○
The assessment question failed to open at starting of exam	○	○	○	○	○	○
Failed to open student record	○	○	○	○	○	○
Showing wrong student record	○	○	○	○	○	○
Failed to get access to the system	○	○	○	○	○	○
After logged in, the system denied to show the account	○	○	○	○	○	○
The system is showing wrong account information	○	○	○	○	○	○

Figure 3.16: Question 13: Respondents experience on the availability of each assets

The question number 13 is showing in Figure 3.16. This question were designed to measure the property *availability* of the system. The answer of this question will help to know how often the user faced the availability problem during using the system. Total 13 statements are used in that question, each statements are related to each assets or the service of the e-learning system. Five point likert scale is used (excluding the option I don't know) to analyze the *availability* of the e-learning system.

Encountered security risk by the respondent The third part of the questionnaire is about the encountered security risk. The topic of the questions of this part are related to the experienced or discovered security risk, un-permitted sharing of copyright materials, experience of false or wrong notification or information from the system.



Encountered Security Risk

Have you ever experienced or have you ever heard about any security vulnerability in the e-learning system? If so, please describe below.

Your answer

Have you ever discovered or have you ever heard about the discovery of any kind of security vulnerability of the system? If so, please describe below.

Your answer

Have you ever experienced unpermitted sharing of copyrighted e-materials?

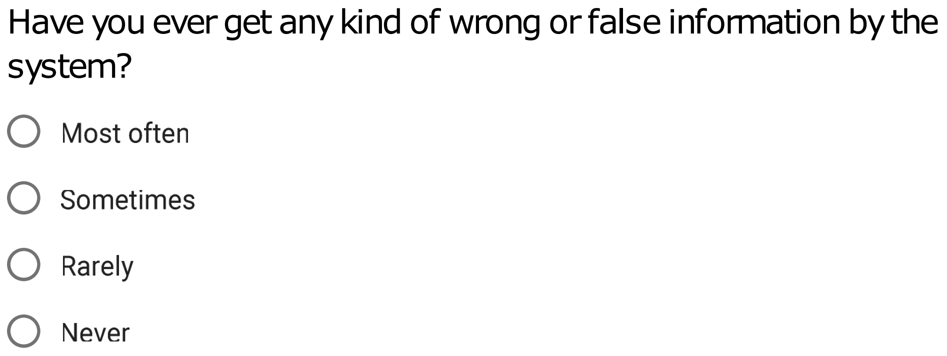
○ I have experienced once

○ I have experienced more than once

○ I have never experienced

Figure 3.17: Question 14, Question 15, and Question 16: Experienced or discovered security risk

Figure 3.17 is showing three questions, which is not mandatory to answer, because it is obvious that this kind of problem may not face daily by everyone. Sometimes someone may experience or discover some security issues in the system, which is an interesting part of this survey. The last question of the figure is about un-permitted sharing of copyright material. A lot researcher may have a lot of copyright material. This question is interested to know if anyone have ever experienced any un-permitted sharing of copyright material by the e-learning system.



Have you ever get any kind of wrong or false information by the system?

○ Most often

○ Sometimes

○ Rarely

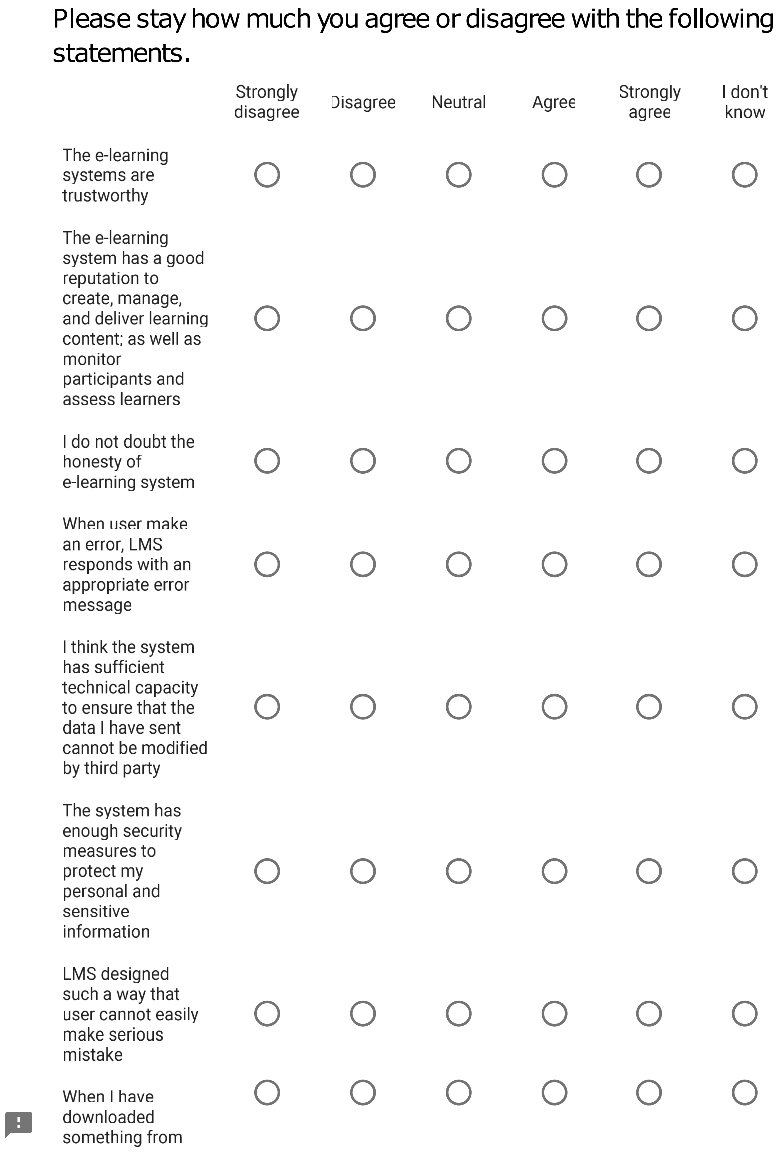
○ Never

Figure 3.18: Question 17: Un-permitted sharing of copyright material and encountered false information getting by the system

Figure 3.18 is showing the last question of the section ‘encountered security risk’. This question wants to know about wrong or false information provided by the system, (i.e. whether this kind of situation is happened very frequently or rarely).

Perceive of security, privacy, and trust This question was to analyze the possibility of inappropriate use of data (perceived privacy), interception of personal and confidential data for wrong purpose (Perceived security), and user’s feelings towards trust to determine the usage of the e-learning system (perceived trust).

This question is designed to know user’s perceived security, privacy, and trust towards the system, showing in Figure 3.19. It has 11 statements based on these three area, and five point likert scale to represent the respondent are how much agree with these statements.

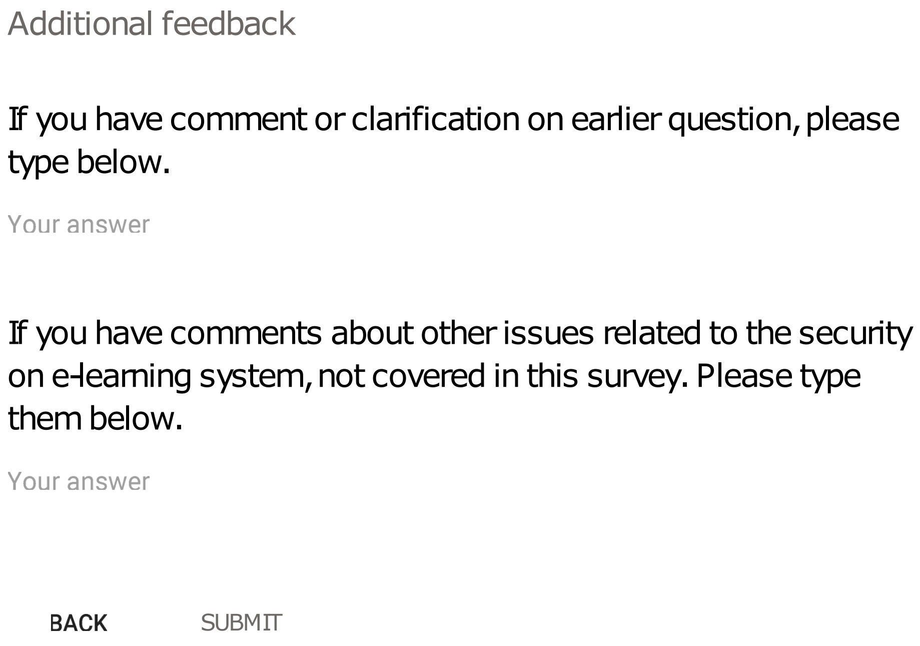


Please stay how much you agree or disagree with the following statements.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	I don't know
The e-learning systems are trustworthy	○	○	○	○	○	○
The e-learning system has a good reputation to create, manage, and deliver learning content; as well as monitor participants and assess learners	○	○	○	○	○	○
I do not doubt the honesty of e-learning system	○	○	○	○	○	○
When user make an error, LMS responds with an appropriate error message	○	○	○	○	○	○
I think the system has sufficient technical capacity to ensure that the data I have sent cannot be modified by third party	○	○	○	○	○	○
The system has enough security measures to protect my personal and sensitive information	○	○	○	○	○	○
LMS designed such a way that user cannot easily make serious mistake	○	○	○	○	○	○
When I have downloaded something from	○	○	○	○	○	○

Figure 3.19: Question 18: Respondents perceived security, privacy, and trust on the system

Closing questions In the closing section of the survey, two questions are kept, showing in Figure 3.20. One is the feedback on the survey, this is not mandatory to answer. Another one is also for some comments on the security issues of e-learning system. As, all the questions above has no comment option under each question, if the respondent may have something extra to tell us, he may use this comment option.



Additional feedback

If you have comment or clarification on earlier question, please type below.

Your answer

If you have comments about other issues related to the security on e-learning system, not covered in this survey. Please type them below.

Your answer

Figure 3.20: Question 19: Respondents comments on the survey

3.3.3 Questionnaire Testing

Before sending to the respondent it is very important to test the questionnaire. The testing ensured that the survey is technically functioning or not, get extra feedback about the survey on wording or necessity of rephrasing, length and timing, and the overall experience of the survey. One recommendation is to conduct an informal questionnaire test among the friends, family and colleagues, before running a test with participant in the target audiences [26].

As survey answering is kind of boring job, it is not possible to ask the participant to be a part of the test group. Again, it is necessary to test the questionnaire first, then solve and update the questionnaire according to the feedback. Some informal test on wording, and technical functionality of the survey is decided to run by the family and friends. Guttom Sindre is asked to go through the survey, as he has good knowledge of the subject matter, and would be able to identify weaknesses of the questionnaire. He gave some constructive feedback and correction, which was solved after getting the feedback from him.

Changes based on feedback According to the feedback, the questions are rephrased. For instance, question 8 wants a ranking of LMS depending on security. In that case, the respondent might not have the idea which LMS is more secure. Therefore, it was rephrased in that way ”Which LMS do you believe is more secure?”. Therefore, the respondent will answer according to their believe. Moreover, this question is not kept as mandatory, as most of the respondent may not have the experience of several LMS, to compare.

Before, the question 9 and question 10 were in the same table, then the respondent had to check two places from likelihood and harmful scale. It was little ambiguous for the respondent. If we divide the question into two parts, then the survey become longer, however the problem of ambiguity will solve. Moreover in Google Form, it is not possible to make a grid table, where participant can check two places of the likert scale. The grid table of Google Form only allows one check in each scale. Because of that, the same table is used twice in the questionnaire with different likert scale. Though this make the questionnaire longer, it resolves the problem of ambiguity and works fine with Google Form.

The Survey was un-anonymous and it requires some personal identifiable information. The information was needed for inviting people for interview. However, it needs to apply to an ethical committee / NSD for getting permission of an un-anonymous survey, before the data collection starts. That would be a reason of delay, and this kind of anonymous survey is sensitive too. Thus, this personal identifiable information part has been dropped, and the survey became unanonymous.

There was some errors in the survey like, some statement which is related to integrity is written in the part of confidentiality. This was also resolved, after getting feedback and revising by the author. Though this kind of error would not affect the survey, because while analyzing and calculating the data, it is possible to write the result in integrity part, which is taken from the confidentiality part of the questionnaire.

Feedback not resulting in changes Some friend said that the survey is long, nonetheless all the questions of the survey are necessary for the research. Thus it was not possible to reduce the number of question and make the survey short. It is made sure that the estimated time for the survey is almost 10 minutes, which is not really too much long.

Some said that it has repetition of statements in Question 9, 10 and Question 11, 12. It is true, as written above, it had one table for both the likelihood scale and the harmful scale, which needs to check in two places of each scale. That time the problem was that, it was ambiguous and Google Form does not support a grid table which allows checks in two places. Thus, it was not possible to make one statement for both scale. As a result, it has to repeat two times for the likelihood scale and the harmful scale. Thus, the survey became little longer as well as it contains some repeated statements.

3.3.4 Questionnaire Distribution

After completing the testing part, the questionnaire distribution has started. For the distribution two media is selected one is email, another one is Facebook messages. Email is used for formal invitation to the survey and Facebook message is used for informal invitation among the family, and friends of different countries from authors network. As the survey is global survey, it needs to recruit participant from different countries. At first, author used her connection from different countries to recruit participant for the survey. Then, the friends of different country from author's network helps to recruit participant by sending the link of the survey via email or some other way to their family and friends from their network. This process helps to get more respondents from different countries. In the email, estimated time is mentioned, keeping in mind that respondents time is important. The estimated time and deadline were also mentioned in the e-mail. Respondent has given almost one week time for filling up the questionnaire, so that they may complete it when they have free time.

3.3.5 Post Questionnaire Work

After the deadline, the result for each respondent is reviewed. The main goal is to understand the respondent behaviour and attitude towards the question of the survey. The result are started to analyze from different perspective and angles. As the response is collected by using Google Form, automatically some results are calculated. As the result will calculate from different angle, the facility of automatic calculation do not use. Because that automatic calculation has two options, one is summary of the total answer, another one is individual answer. In the summary of total answer, the results from all the countries and LMSs are showing in same charts. Despite this, the research needs to organize the result of each country and each LMS. In order that, the author has to calculate manually all the answers with respect to country and LMS. For calculation, Microsoft Excel is used. Different methods are learned from different literature, which helps to know how to analyze the questionnaire data, and how to get result from the data.

3.4 Interview

Interview helps to get deeper understanding about the subject. It is possible to get qualitative information, which is impossible to get by survey questionnaire. It is not possible to get inside of each question through the questionnaire however interview works fine in that case.

After getting an answer of a question from the interviewees, it is possible to ask further question about the topic. For instance, why he thinks like that? If he tell about a new problem, then it is possible to ask why this problem occurs or how to solve them etc.

Three different type of interviews can be conducted to a single person. They are Fully structured, Semi-structured, and Unstructured [26].

Fully-structured A set of predetermined questions were asked to the interviewees in order and there is no room for improvisation or follow-up [26], [29].

Semi-structured There may have some predetermined question set, known as *interview guide*; the wording of question may vary. There is room for discussion and based on the discussion topic. Other theme can be included to the interview [26], [29].

Unstructured No pre-structured questions are prepared for the interview, however has a theme for discussion, and the interviewees leads the conversation [26], [29].

For the structured interview, the person who is conducting the interview does not need to have any knowledge about the topic. Nevertheless for semi-structured and unstructured interview, it is important to have a good knowledge on the research topic [29].

This study required a semi-structured interview, because it is more flexible and the author was not that much familiar with the inside of the security issues of the e-learning system of the university. Hence, semi-structured interview guide or questions are set up for the interview, so that the interview has a room for discussion, which may lead the discussion to a new interesting direction. At the same time, the interview has a clear goal with the discussion.

As the plan is that interview would be taken from some expert or experienced person of the e-learning system, Guttom Sindre referred a person for the interview, who has experience of working with Blackboard in NTNU. That person is able to provide a lot of information about the inside of the Blackboard, and share his working experience. After interviewing that person he suggested two more person who is fitted for the interview and may have some good knowledge about the research area.

3.4.1 Interview Guide Design

Interview guide is a document which is prepared before conducting interview, which helps to support the interview containing with the areas of the research interest, sample questions, and relevant prompts. Thus designing interview guide is one of the most important task which should prepare properly before conducting the interview. Important factors of interview guide are covered below.

Question order For a novice interviewer it is challenging to design an interview guide to ease the interview process [30]. It is important to make the interviewees feel comfortable and easy while conducting interview [31]. It is recommended to start with "small talk" related to his working experience before starting the question from the research area, so that he may feel comfort to start a conversation with the interviewer [32]. The author is the interviewer of the conducted interviews and she has no previous experience of conducting interview. Reading about how to conduct an interview can not make herself expert in conducting interview, however at least she knows the theory of it. At the starting of interview it is important to set some warm-up questions so that the interviewees get a chance to express himself without thinking too much. Hence, the interview guide of this study starts with the question *Could you tell me a little about your day-to-day work?*. This question can also help the participant to start the conversation for a couple of minutes without any interruption. As a result, the interviewees may start feeling comfortable in the conversation. Then main questions of interview which is related with the research question are kept. That part asked about the interviewees' experience in security issues, which is an interesting subject of this research. Then the questions related to the shifting from monolithic system to modern e-learning ecosystem and there increased opportunity and threats are kept in the design of the questionnaire. The closing part is kept for some comments like if the informant have something more to tell us about the subject which was not asked in the previous questions yet maybe interesting for the research can tell it in that part. As the questions are made quite open, the discussion of that part could lead to the other direction or theme related to the security of e-learning system. In that part, interviewees also asked some questions to the interviewer to understand what the interviewer really wants to know or what part of security is focused in that research. After getting that the interview questions are open and they may discuss about anything of the research, the interviewees tried to tell something more from their experience which might be interesting for the research.

Question phrasing The wording of questions can impact the answers given by the interviewees. It was important to make the phrase of the questions in a conversational way. Clarify the question that might be vague or confusing. After designing the interview guide, it is reviewed by Guttorm Sindre, and he gave some correction. On the questions there was some direct questions which might not make the interviewer comfortable to answer. Therefore, the questions are rephrased by including the phrase like *what do you think or believe*, so that the participant may answer from their experience. Guttorm Sindre also suggested me to send the interview questions to the interviewee before conducting the interview, in case they face any problem in understanding the question or there need rephrasing of any question, that can be solved before the interview. The wording of question are designed by keeping in mind that the interview is semi-structured and the answer may go to many direction. The question could be altered in each interview depending on the conversation.

Questions properties The properties of a question can affect the answer. There are three properties, which can impact the quality of questions: open questions, leading questions, and double-barreled questions.

Open questions are formed in that way so that the participant cannot answer simply yes or no, but talk about the topic in depth. It anticipate follow-up question for moving up the conversation along [31].

Leading question can show the interviewers opinion to the informant, which might change how they answer. This kind of leading question should be avoided by modifying the wording of the question. Though it might be challenging sometimes [31].

Double-barreled questions are where multiple questions are put together, which should be avoided. As they can be difficult to answer and cannot be answered fully [33], [34]. If the informant miss the answer of the part of the question, then it can be added in the follow-up questions. However, this kind of questions should be divided into more than one question so that the informant could answer one by one question.

Though the questions were open questions, the interviewer once got kind of simple answer like *yes or no* while conducting the interview, because the informant do not faced any security issues during their work. However, in the questionnaire-guide there is some follow-up questions which has some more questions like *what are the possible security threats in the field where you work?*. Then the informant talked in a little about the subject.

In the designing face of questionnaire, leading questions are rephrased and there was some double-barreled question which was divided into more than one questions. For instance there was a question like *what are the advantage and disadvantage of monolithic and modern e-learning ecosystem?*, which was divided into two questions to keep the question simple. Otherwise the responded may miss other part of the question while answering.

Probes and prompts After answering a question there might be a need for elaborating the topic. Probes are the statements, a set of questions, or signals that encourages the participants to go deeper into the topic, or present the reasoning behind the statements. Commonly used probes are:

Continuation probes helps the participant to continue talking on the same subject by saying ”Mmh” or repeating the last statement [35].

Elaborating probes helps to elaborate the subject more by saying ”Could you tell more about ...?” or ”Could you give example of ...?” if the interviewer need to know more about the subject [35].

Clarification probes helps to clarify the opinion provided by the informant, by asking ”Could you give more context on...?” or ”Could you rephrase ...?” in case of any opinion is unclear to the interviewer [35].

Prompts are the set or the range of possible answers that the interview expects from the informant. The list of possibility can be showed by a ‘prompt-card’, or can be read out by the interviewer [26].

The interviewees have used the ‘elaborating probes’ while answering the questions. For example, they used ‘Mmh’ and also sometimes they have repeated the last statement. Sometimes, to express something they have start a sentence and then stopped and altered the sentence in another way to express the subject in a better way. The interviewer also used the ‘elaborating probes’ and ‘clarification probes’, when needed. More details of probes and prompt of the interview are written in the next Section 3.4.2.

Interview duration A long interview may discourage the participant. Thus deciding interview time duration is important while planning the interview guide. Considering a full hour is too long and half an hour is short time. Including 5 minutes for warm-up question and 5 minutes for formalities; 45 minutes is decided estimated interview time. Keeping this in mind, the interview guide is made, so that it may not take more than 45 minutes. It facilitates to tell the informant that only 45 minutes in total would be needed to take part in the interview while inviting them, which may encourage the participant to take part in the study.

Though it seems it will take 45 minutes, two interview takes about 45 minutes and one interview takes 25 minutes. The duration of the last interview was short, comparing other two interviews, because the informant do not have enough information to tell unlike other two informant.

Sending the questionnaire before the interview While inviting people for the interview a list of interview questions are sent to the participant, so that if they do not understand any question, the interviewer can get a chance to rephrase it before conducting the interview. It also helps the informant to prepare for the interview from before, as they are aware of what will be asked in the interview. As a result, while conducting the interview it seems that the informant were quite ready and confident. Also, no extra time needed for any other extra thing. However, another informant was too busy in his work and meeting that he did not even get time to open it. However, he also gave a lot of interesting information for the research.

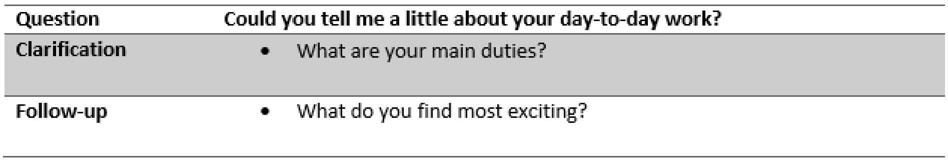
3.4.2 Interview Setup

By using the above theory ‘interview guide’ is designed, which is represented in this section. Each question is associated in a way that there could have chance to elaborate the topic and possibility go to the depth of the topic.

The questionnaire of interview has started with warm-up question. In the main body of interview questionnaire there is questions on participant’s security experience, security issues may involve in the system, the assets of the system, and security threats. Another most important question of this research are about shifting from traditional monolithic to modern e-learning ecosystem and the increased opportunity as well as threats in security. The questionnaire ends up with a closing part which is kept for more comments from the side of both informant and interviewer.

General information A general information about the interview is given to the participant, at the time of inviting the participant for the interview. While the participants are agreed to conduct the interview, the questions of the interview is sent to them, to make sure that they understand all the questions. If there need any rephrasing in the questions then rephrase it before the interview. This also helps the informant to get an overall idea about the interview. The permission of recording the interview, is also taken from the participant before the interview, as recording of the interview is also an essential part for the transcription the interview.

Warm-up questions As described above the goal of warm-up question is to make the informant comfortable in the conversation.

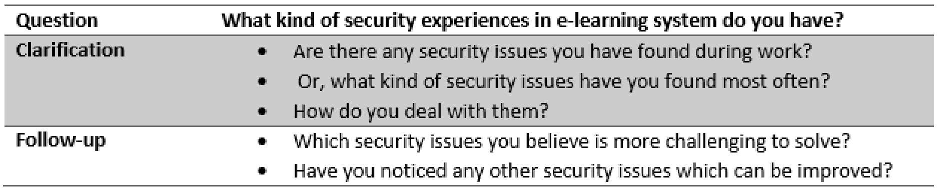


Question	Could you tell me a little about your day-to-day work?
Clarification	• What are your main duties?
Follow-up	• What do you find most exciting?

Figure 3.21: Question 1: Warm-up question

Figure 3.21 shows the warm-up question, which provides the opportunity to talk about their work, which is an easy start for the participant to talk for 2 to 3 minutes without interruption. If the participant do not have a lot of thing to say, then simple prompts such as asking main duties or what they find most exciting could be asked. From the answers of the participants it comes to know that the three interviewees are working on three different part of the e-learning system of NTNU. The another advantage of that question is that the interviewer get to know about the type of their work, as the following questions is related on security experience of the informant. In case the informant did not face any security issues while working, it was possible to ask if there is any possible security threats may encounter in the field where he is working.

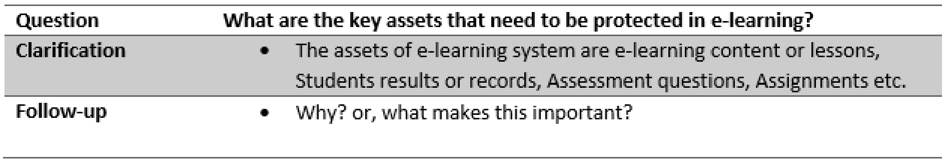
Security experience One of the interesting area of this research is to the participants findings on security issues during work.



Question	What kind of security experiences in e-learning system do you have?
Clarification	• Are there any security issues you have found during work? • Or, what kind of security issues have you found most often? • How do you deal with them?
Follow-up	• Which security issues you believe is more challenging to solve? • Have you noticed any other security issues which can be improved?

Figure 3.22: Question 2: Participants security experience

Figure 3.22 is showing the question 2, which asks the participant about their security experience. The elaborating probes are, whether they find any security issues while working in the system, if so, how they deal with it. If participant has a lot of experience then what are the more challenging issues the participant believe. The answers of the participant is noted down, and then brought up when talking about the topic. Moreover, the question can be changed depending on the answer of the participants like if there is any other security issues which can be improved or how the issues are solved etc.

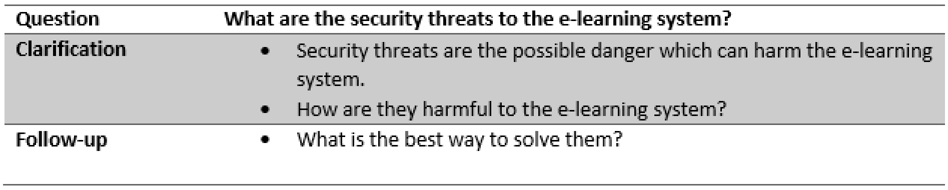


Question	What are the key assets that need to be protected in e-learning?
Clarification	• The assets of e-learning system are e-learning content or lessons, Students results or records, Assessment questions, Assignments etc.
Follow-up	• Why? or, what makes this important?

Figure 3.23: Question 3: Key assets of the e-learning system

Security issues Figure 3.23 is showing the question 3 of the questionnaire, which is about the key assets. In that part, the main question which is asked to the participant is about the key assets that need to be protected. The prompts of some assets are given there in the clarification part of the question. The answer on the key assets are noted down, and from that it is asked why he thinks that the key assets are important. The answers of that question varies from the perspective of informant, for instance the informant who is dealing with the examination of the e-learning system says the most important assets are grading or student record; however another informant thinks personal information is most important which is related to the authorization process.

Security threats In that part, the question will be asked about the possible security threats of the system, showing in Figure 3.24.



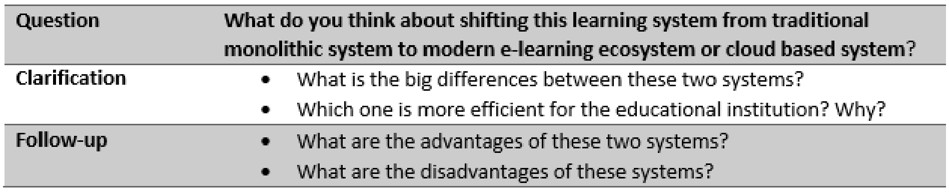
Question	What are the security threats to the e-learning system?
Clarification	• Security threats are the possible danger which can harm the e-learning system. • How are they harmful to the e-learning system?
Follow-up	• What is the best way to solve them?

Figure 3.24: Question 4: Security threats of the system

The participant answers from his believe about the possible threats of the system. To clarify the answer it would ask to the participant that how the mentioned threats are harmful to the system. If the participant has any clue how to solve the threats he would tell about it.

Shifting from traditional monolithic to modern e-learning ecosystem This question and next two questions relate to the second research question of this research. These are another interesting part of this interview.

In the question 5, showing in Figure 3.25 wants to know informants opinion on the shifting from traditional monolithic system to modern e-learning ecosystem. The elaborating probes of that questions can be asked about the differences between two system or, which one is more efficient and why. While answering this question the

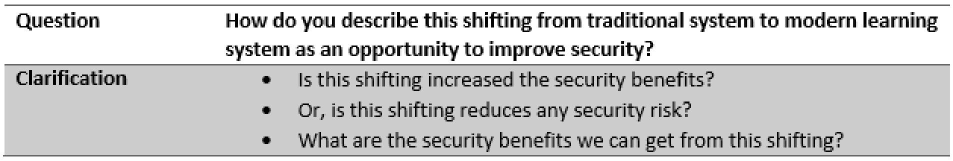


Question	What do you think about shifting this learning system from traditional monolithic system to modern e-learning ecosystem or cloud based system?
Clarification	• What is the big differences between these two systems? • Which one is more efficient for the educational institution? Why?
Follow-up	• What are the advantages of these two systems? • What are the disadvantages of these systems?

Figure 3.25: Question 5: Monolithic system vs modern e-learning ecosystem

advantages and disadvantages of this two system will come out from the participant. If they do not mention about the advantages and disadvantages of these two system, while answering it can be asked as follow-up question. In some cases it was found that the interviewees do not like to answer that question as he knows the main focus of this study is security. If it is found that the interviewees is not able to answer that question, the question is skipped and shifted to next question.

Security improvement by this shifting: The next question of Figure 3.26 wants to know whether the shifting increases any opportunity in security.

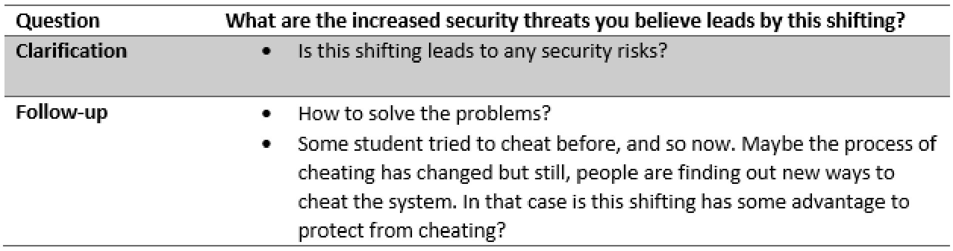


Question	How do you describe this shifting from traditional system to modern learning system as an opportunity to improve security?
Clarification	• Is this shifting increased the security benefits? • Or, is this shifting reduces any security risk? • What are the security benefits we can get from this shifting?

Figure 3.26: Question 6: Shifting increases the security opportunity

The participant can describe the security benefits from his perspective or experience. To know more it can also be asked that 'do the shifting reduces any security risk?'

Increased security threats by this shifting: This question wants to know whether the shifting leads to any security threats to the learning system. The participant can answer about a list of security threats lead by this shifting. The participant can give a solution from his perspective for the threats. The question is showing in Figure 3.27.

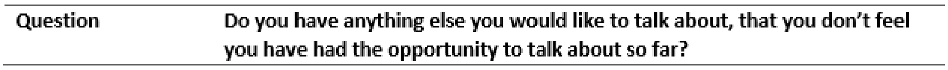


Question	What are the increased security threats you believe leads by this shifting?
Clarification	• Is this shifting leads to any security risks?
Follow-up	• How to solve the problems? • Some student tried to cheat before, and so now. Maybe the process of cheating has changed but still, people are finding out new ways to cheat the system. In that case is this shifting has some advantage to protect from cheating?

Figure 3.27: Question 7: Shifting lead to security threats

If the participant do not find any scenario to describe security risk than the prompts is also given in the question, which is about cheating in the exam. Considering that situation the participant gave the answer of above question. Sometimes it seems that this part is not possible to used as a scenario to describe the answer. When it seems that this follow-up questions can not be linked with the answer of the interviewees than the follow-up question is used as a new question. The answer of that new question was changed into the security advantage-disadvantage, possible threats, some cheating experience of e-exams of the system.

Closing question At the end of the interview Figure 3.28 is showing the last question.



Question	Do you have anything else you would like to talk about, that you don't feel you have had the opportunity to talk about so far?

Figure 3.28: Question 8: Closing question

It is important to give room to the participant to say something, which is outside from this structured question yet relevant to the subject. While discussing a topic it is possible to miss, or not to recall something by the participant. Sometimes the interviewer also wants to ask some extra question from the previous answer of the participant. Hence this closing question gives the space to discuss that kind of topic. While conducting interview if the interviewer found something interesting, this gives the interviewer to ask some extra question on that interesting subject or area. While answering this part the participant seems more comfortable than before, as there is no fixed question. Therefore they tried to give some extra information from their knowledge so that the interviewer can get something more for her research.

3.4.3 Conducting the Interviews

To make sure interviewees are comfortable and willing to share information, several factors are taken into account. The main factor which are considered in this study are presented below.

Interview skills Skills are involved with practice, just reading about interview can not make anyone good interviewer. It is not feasible to expect from a student to be an expert interviewer in the short time of master's thesis. Again, it is important to be aware of skills to get value as an interviewer.

A good listener can move forward the interview, as well as a good memory helps to tie together strings from different parts of the interview. Having a clear mind can simultaneously conduct the interview, taking notes of the interview, and formulating next question, are considered as a central skill of an interviewer. A curious mind and strong interest in the field of questions consider as a quality of a good interviewer [26], [31]. The author is the interviewer of the research and she has no experience of conducting interview, though she was aware of the interview skills to continue an interview. The theory of the book [26] helps her to get value as an interview. While conducting interview, many kinds of situation occur like one question wants to know about the security experience of the interviewees and the interviewees did not have any security experience. This situation is handled by asking bit different question like what are the possible security threats of the system, he believes?

Interviewees This research needs some experts who are involved in managing the e-learning system so that they can give some deep knowledge and information for this research. As they are working with the system they have enough experience with the technical things.

In total three interviews has been conducted, among them one informant worked with the functionality of Blackboard, to make sure that teachers could use the system, but not directly responsible for the security. The second informant is in the charge of the project for electronic exams which are the part of the LMS. The third interviewees has the position of coordinator of the Blackboard LMS at the faculty. The three interviewees are working in the three different parts of the Blackboard, and they have shared security issues related to the system from their experience and perspective.

During the interview, sometimes the informants used some technical terms or mentioned some name of well-known software which they are using regularly and the interviewer was not familiar with that. Then the interviewer asked about the term or the software and come to know about that. After clearing the term, the discussion continues, which helps the interviewer to understand the conversation. At the end of the interview, some more conversation continued, which are from informants curiosity about the research and then they tried to give some more information which might helpful for the study.

Participants putting on a front There may have some situation where the participant were telling a story of something else which is not related to the topic. In that situation there is less likelihood to give relevant answer by the participant. The recommendation is that to stop asking follow-up question, and try to rephrase the question in a way that there is no chance to misunderstand the question [35]. This kind of situation also occurred during the interview, and the theory is followed to handle the situation. When it seems that the informant do not have enough to tell about the topic then the next question is asked.

Recording Semi-structured interview without making recording of the conversations is an impossible challenge. A lot of vital information can lost in that way. Interviewer makes notes and forms next question to the interviewees during the interview, hence it was not possible for interviewer to note each important point. After the interview it is not possible for the interviewer to memorize the whole conversation. Therefore, recording is must in that type of interview. The recording will help to analyze the result after interview. Though making recordings of the interview is also challenging, as the interviewees might see this as threatening, he may less honest in his conversation in a fear that the recording might leak, and the worst case might cause the participant to withdraw [30]. In this case the interviewees were not fearful yet most of them did not tell any current security issues, they just told some previous issues which is already solved. They may not aware of any current security issues or may have some current issues but do not want to share it because it may be threatening for the system if they leak the information.

Note sheet Taking notes during the interview is also very important. It is also considered as backup while recording are lost, or unusable. Taking notes also increases the attention towards the participants answer. It was not possible to write whole sentences while making notes as well as listening the interviewees. Therefore main points are written down in the notes. The points also helped the interviewer to ask further question, which was not possible to ask by stopping the interviewees while he was answering another question. Therefore, the notes helped the interviewer not to forget the question which will be asked when the interviewees complete the answer of current question.

Location and scheduling It is important that the interviews are conducted on the participants' term, as the interviewees are the busy people, under no obligation and with little incentive they are participating in the interview. If the location of interview is in the place of interviewees' office than this known environment of the interviewees will help them to feel more comfortable and relax during interview [32]. However the possible problem is the environment might have interruption or some other distracting factors and there might have a lot of noise, which makes the recording as well as the interview process difficult [36]. Most of the interview of this research are taken place in the interviewees' office, and luckily there are no noise which may create problem in recording. One interview did not place in the interviewees' office and the recording of that interview has some noise though it was not that disturbing to transcript the recording.

For planning the interview schedule, a lot back and forth communication are required. The interviewees of this study are busy people, and taking part in the interview is a voluntary task for them. After agreeing for the interview, the participants gave their available time and they decided the location of the interview and that is there work place. Different participant gave different date for interview hence there was no chance for collision of schedule.

3.4.4 Post Interview Work

After conducting all the three interviews, the post work begun. The main activity of this part is transcription and coding, which are described below:

Transcription From the audio recording and notes of each interview, data are extracted, and written word by word. This process is called transcription. To do this, high level of concentration is required for extended period. It is a time consuming process. One common pitfall is misinterpretation of the recording or mistyping of interviewees' statements, which may change the meaning of the statement. This distorted data can damage the final result. To avoid this, the researcher personally can transcribe the interview [36].

To record the interview, recorder of smartphone is used. Luckily the voice quality of recording was good enough to listen, while transcribing. The transcription process are started immediately after conducting the interview as the conversation of interviews are fresh in memory at that time. No transcription software is used in this process, all the process are done manually. From the audio recording the conversation were typed or written by hand. An one hour interview takes 9 hours of transcription. Repeated listening of the recording are needed during this process, to get deeper understanding of the context. Because of that, this process took that long time.

Coding From the raw text of transcription, finding out the research topics and concepts are called coding. Related topic and context are marked in the text of transcription, usually with a code. The text is processed and anything related to the specific topic is marked with the same code. Now, this can be extracted from all the interview and processed separately. The coding process should be done in a correct way because it shapes the data that can be retrieved from the information at hand. At the time of coding, if a concept is not identified then it will not possible to investigate further and will affect the conclusion [35].

Coding process starts by reading through the text of the interview, note down the frequent occurring or interesting topics and quotes. The topic is identified - using the notes, literature, questions of interview guide and common sense. It is recommended to make a list of topics to attempt to find a new topic like the connection between the existing topics. As the coding process is depending on the research questions, the research questions are kept in front while making the list of topics. After making a list of the topic, it is important to make a clear and consistent definition of the topic and make the codes which will use to mark up the text. One recommendation is to define the code as such [35].

- What is it called or define?
- How will it be recognized?
- What will be excluded?
- What is a good example?

The definition of coding, showing in the table 3.1 are made based on the research question. The definition will use through out the coding process and should not change throughout the process. It is recommended that the definitions are tested on a sample of the text to check if the definition hold up [35].

#1 Key Assets

Definition: The assets which has high value to its stakeholder and the attack on the assets will create a huge loss to the stakeholder.
Recognition: Give a list of key assets which need to be protected, discussed with reasons.
Exclusion: The assets which has low value will not discuss here only high value assets are discussed here.
Example: Informant will tell about the key assets of the system with some reason from his perspective.

#2 Security Issue

Definition: Security issues are the possible vulnerability and experienced attacks in the e-learning system, or the security challenges the informant are facing currently.
Recognition: Talk explicitly about the security risks and threats, which have been found during work, challenging security issues exist in the system, and how the issues are solved or could be solve.
Exclusions: The security issues which will not related with the technical side like bribing employee to get confidential data is not part of that issue.
Example: The informant share his thoughts about the possible threats of the part he is working in the e-learning system, and if the problem occurs how to solve them as well as their exposed security experience of the e-learning system (e.g. hacking, or getting abuse mail) and how the problem has been solved.

#3 Cheating in the Exam

Definition: Breaking regulation of exam in wrong purpose to make better grade is the cheating in the exam

Recognition: Talks about prevention steps, possible cases, technical and non-technical solutions, experienced scenario.

Exclusion: The attack on the examination system which is not related with cheating in the exam are not discussed here.

Example: The informant will describe from his experience about how cheating in the exam occurs in the system.

#4 Shifting from monolithic to e-learning ecosystem or cloud architecture

Definition: A brief discussion on the shifting from traditional monolithic shifting to modern e-learning ecosystem.

Recognition: Talks about both the system and their differences, how the shifting helps the learning process and what are the problems of this shifting.

Exclusion: Security is not included here, more general information about the shifting is collected here.

Example: Informant can share his opinion about the shifting, what are the differences he found in the system as well as the advantage and disadvantage of this shifting.

#5 Security benefits of shifting

Definition: The opportunity to improve security of this shifting from traditional system to modern e-learning ecosystem.

Recognition: Talks about the benefits in security leads by the shifting as well as the risk which has been reduced by the shifting.

Exclusion: General increased opportunity is excluded. The increased security threats of this shifting are not described here.

Example: The informant describes the security benefits or reduced security risk of this shifting from his knowledge.

#6 Increased threats leads by this shifting

Definition: The security risks which might increase by this shifting.

Recognition: Talk about the increased security threats or other security problems leads by this shifting with some reasoning.

Exclusion: Only security threats are included, general disadvantages are excluded.

Example: The informant will describe what are the threats or security risk might increase by this shifting as well as how this shifting is harmful in some specific area.

Table 3.1: Topics identified for coding

After making the definition of each topic, the interview text documents are marked up. By going line by line or partial line the document is marked up and give a name to each marked up line or partial line. A table showed in Table 3.2 was made from the marked topics with respect to the interviewees and it was make sure that all the marked topics from the document are included in the table. The given name of all marked line and sub-line are included in the table with respect to the informant. In that table similar topics are kept in same row. Here one column is kept for one data document. This study has three data document of the three conducted interviews.

First row of the table are representing the experienced issues which are discussed by the informant. Second row is about challenges they are currently facing, third row is about the key assets, fourth row is what are the threats are discussed by them, fifth row is the opinion about shifting from traditional monolithic e-learning system to modern e-learning ecosystem, the following rows are discussed topic about increased security benefits and threats by this shifting, the last row is about the discussed topic of cheating in the exam.

Table 3.2: Initial themes from interviews

Informant X	**Informant Y**	**Informant Z**
Experienced issues: trade-off between functionality and security, phishing attack	Experienced issues with different kind of software	Experienced issues - violation of authorization using session cookies
Challenges in re-design the LMS (Blackboard)		
Key assets- student records, student's work, personal information	Key assets- student records, student's work, personal information	Key assets- student's work, personal information
Threat- Loop-hole that enable cheat in the exam	Threat- DDOS, identity theft, make confidential data available	Threat- unauthorized access. Solution-feide
Integration in monolithic and ecosystem	Limited control over infrastructure and configuration in e-learning ecosystem	
Shifting focuses on probability rather than security benefits		
Difficult to find and solve security holes in the e-learning ecosystem.	Making changes will be difficult if the system has too many customers	
	More exposed for attack, and attack on someone could influence other	Increased security threats of shifting- Access and verification problem
Cheating experience	Technical solution vs non-technical security solution	

From the Table 3.2 some more tables are made, where first column holds the major topic that are constructed from cluster of comparable ones and the name of first column is 'Primary theme'. The second column holds more unique topics, which seems important to research topics or research purpose. The name of the second column is 'secondary themes'. The third column is kept for the quotation of the informant related to the themes. The tables are discussed in next Chapter-'Result' and showed in Table 4.8, 4.9, 4.10, 4.11, 4.12, 4.13. In that chapter detailed discussion about the interview topic are discussed.

3.5 Alternative Methods

The chosen research methods of this study were the online survey and individual semi-structured face-to-face interview. There are some other methods which could be used for this study, and the reasoning of not using those other methods are briefly discussed below.

Group Interview The group interview is another type of data collecting method where a lot of informants present while conducting the interview. Group interview are useful to get detailed information about personal and group feelings, perception, and opinion as well as it has ability to offer a broader range of information. One advantage comparing to individual interview is that group interview can save time and cost.

For this study, group interview is not selected as a research method. The reason is that, there is not a lot of informant available for this study. One person has been found who is fit for the interview, after conducting the interview he suggested two more person who can fit for this interview. As they are busy person they gave time according to their schedule, and the scheduled date were different. There are some other reasons not to choose group interview as a method. As the participants are from almost the same field there can be disagreement or irrelevant discussion which can be difficult for the interviewer to handle or to turn them back to the subject.

Case Studies Yin [37, p. 23] defines the case study research method "as an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used". There are several challenges involved in this case study method. The main obstacle is time, as a master's student, this study has limited time. The entire process from identification of need, to delivery and evaluation of the product, would not have been possible within this limited time. This study is conducted only in NTNU, Trondheim, having a lot of universities in Norway, which is reducing the number of possible area. Moreover, performing this kind of research would also run the risk of changing the behavior of the participants, as they are providing inside of the security issues related to the e-learning system. This will produce a very weak result for this study, thus this method is not considered for this study.

Delphi Method Delphi method [38, p. 3] is "a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem". The respondents answer the questionnaire two or more than two rounds. Between the rounds, the questionnaires are revised based on the response from the previous round. During the process, the range of answer is decreased and the group is converged towards the 'correct' answer. After a predefined criterion, the process stops and the mean or median scores of last round figure the result [39].

This method is time-consuming as the master's student has limited time this method is not well suited for this research. Moreover, the respondent may not feel interested in participating in this kind of method. There may have schedule clash among the participant hence it may not be possible to gather all the participants in one place at a time to do this Delphi method. After two iterations the process might have to be stopped because the participant would not take part further round.

3.6 Conclusion

This chapter starts with representing a diagram of research process of this study. Research question defining was the first activity of that research. After defining the research area, research methods are decided for this study. Section 3.1 describes 'Research Question and Choosing Methods'. This section shows advantage and disadvantages of different methods and the reason for choosing selected method to collect the answer of the research questions of this study. Section 3.2 'Participant Recruitment' explains how participants were recruited for this study. A detailed description of questionnaire design, questionnaire setup, questionnaire testing, distribution of questionnaire, and post-work are given in Section 3.3 'Questionnaire'. Again, a detailed explanation of the design of interview guide, interview setup, conducting the interview, and post-work are described in Section 3.4. There are some other methods, which could be used in this research. A brief description of that methods are given with the reasoning of not using them in this study are discussed in Section 3.5.

Chapter 4

Results from Evaluation

This chapter presents the result of the study as well as give an overview of security in e-learning system to the developer to improve the system. As the study is performed by the mentioned two methods, the result of the two methods is presented here. This chapter starts with participants demography for both of the methods. Then the result of the 'questionnaire' are described first, the result of the 'interview' are described later. The chapter concludes with a description of the limitations of the study.

4.1 Participation Demographics

It is important to get an understanding of the participants in this study to interpret the result. There are several stakeholders in e-learning system, however for the *questionnaire* part students are the key stakeholder to analyze their view towards the system and for the *interview* part the employee who is responsible for managing the system are the selected stakeholder. As the students are the main user of the system, and they can give feedback about the security issues they have been faced and the expert is able to provide the inside of the system.

4.1.1 Number of Participants

For the *questionnaire* part this study has focused on the global stakeholders. From the wider distribution to all of the countries this study has selected five countries. The countries are Norway, USA, Canada, Malaysia, Bangladesh. The reasoning of selecting this country is discussed elaborately in Section 3.2. On the other hand, the participants of the *interview* part are the responsible people of managing the LMS, *Blackboard* in NTNU. Comparing to the number of studies of a university the number of the employee who is managing the e-learning system is very low. Among the employee, only the people who have experience with security are the participant of the interview part. This is the reason of getting only three participants. Moreover using questionnaire is easy to get global participant, nonetheless it is not that easy to conduct the face-to-face interview. Hence, for *questionnaire* part the participants are from different universities from five different countries and for *interview* part the participants are only from one university. Because of that this study got seventy-six participants for *questionnaire* and only three participants for *interview.*

Different kinds of participants are responded in *questionnaire* while the same kind of participants is participating in *interview.* Thus it is important to understand the participant of *questionnaire* statistically. Below statistically country-wise and the LMS-wise number of participates in the questionnaire are showing and describing briefly.

Country-wise

The number of participation among the five countries are showing in Figure 4.1.

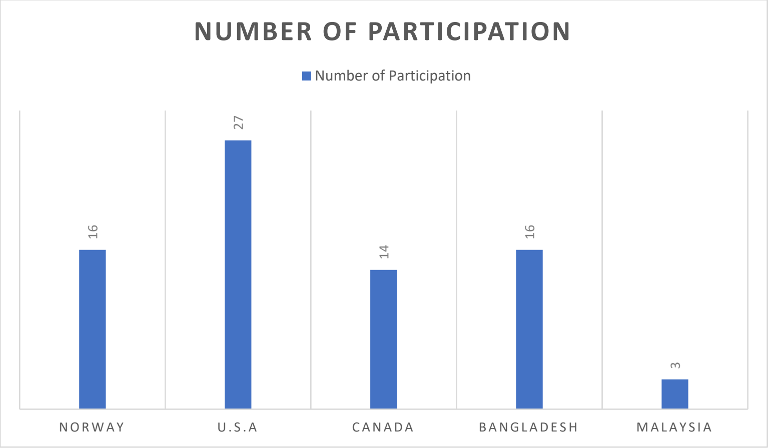


Figure 4.1: Participant rates from different countries

This figure is showing that only 3 respondent are found from Malaysia for this study. The reason is that the author has only two friends there in Malaysia. They could not use their network that much to spread the survey among their friends. In the testing phase, it is found that this study would not find enough participant from that country. After the testing phase, the questionnaire was distributed only the remaining four countries. The bar chart is showing that maximum participants are from the USA, this is because the authors maximum family member are in the US, and her cousins are the student of different universities of US. Therefore, they helped a lot to spread the questionnaire among their friends. Bangladesh is authors native country, where she has completed her Bachelor. Some of her friends are responding to the survey from Bangladesh. 16 people from Author's network in Norway are responded to the survey. The author also sends some more email to other students who was her classmate in the different courses in NTNU, nevertheless very few responses are got from there.

LMS-wise

Among the participants how many students are using which e-learning system is showing in the bar chart of Figure 4.2. From the total 76 participants, several participants have experienced with more than one e-learning system. Because of that here it is showing that the total number of respondents is 86, while total number respondents are 76.

Maximum participants from each country are using Blackboard, except Malaysia, they are using *I-taleem* as LMS. The educational institution of Norway are using *It's learning* and *fronter*. However, from this year NTNU has started to use *Blackboard*. Canada and USA are mostly using *Desire to learn* as their learning management

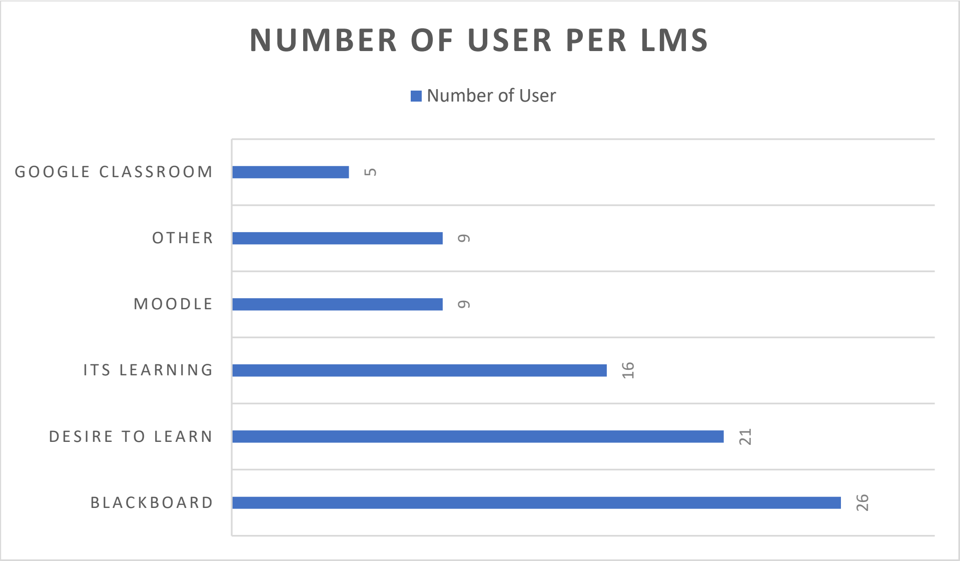


Figure 4.2: Number of user in each LMS

system, as well as some institution of Canada and USA are also using *Moodle* and *Canvas*. Most of the Bangladeshi educational institution do not have this kind of learning management facility, yet their learning management system can register the student for the courses, and show the results or records of each semester. For this kind of administrative work, the educational institutions are using a system called *IRAS*. Though few participants from Bangladesh responded that they are using *Blackboard*, *Google Classroom*, *talent LMS* as LMS or e-learning system.

4.1.2 Security Awareness of Participant

While using the e-learning system some people are thinking about security, while some are careless about security. To understand the security awareness among the participant the question of Figure 3.9 is designed in the questionnaire and the result is showing in Figure 4.3.

Among the 76 participants, 8 are not thinking about security at all, where 13 are always conscious about security. Almost 59% participants are conscious about security, if we consider the scale *always, very often, sometimes* as the positive rating (i.e. conscious about security) and *rarely, never* as the negative rating.

E-learning system do not contain that much personal and sensitive information, this could be a reason for choosing *sometimes* and *rarely* by most of the participants. On the other hand, some students are serious about the security of their information whether their learning activity are tracking or the given personal information are safely stored and retrieved. Because of that some students might choose *always* and *very often*. Hence this result shows that students are conscious about security while using the system.

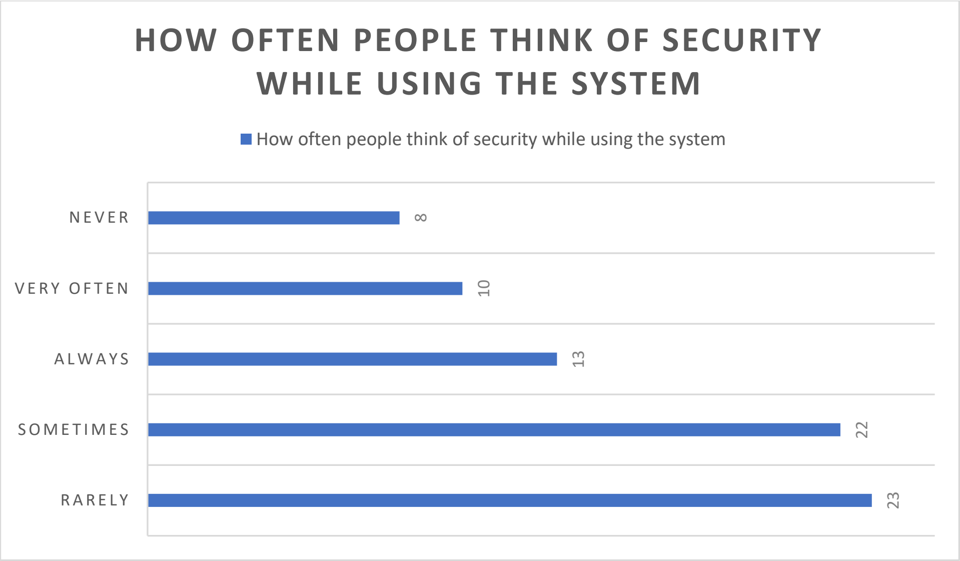


Figure 4.3: How often people think of security while using e-learning system

4.2 Satisfaction on Security

Among the 76 participants from the considered five different countries, the scale of satisfaction varies from participants to participants. We have considered five scales to identify participant's satisfaction, they are *very-satisfied, satisfied, neutral, dissatisfied, and I don't know.*

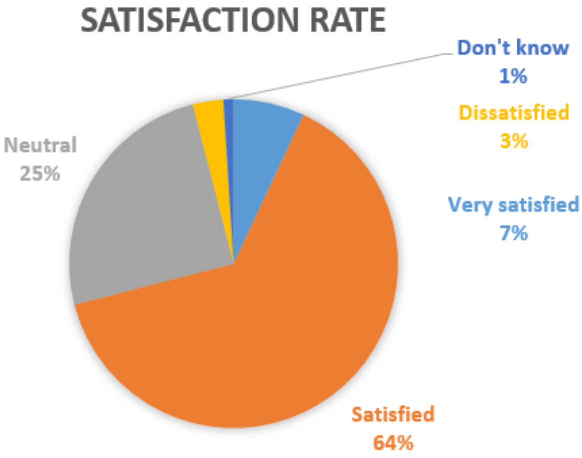


Figure 4.4: Satisfaction-rate among the user of different e-learning system

The result of satisfaction rate in the security of e-learning system among different countries is showing in a pie chart of Figure 4.4. Which shows that most of the participants are *satisfied* with their LMS and one-fourth of the participants are *neutral*.

4.2.1 Country-wise Satisfaction-rate

We are considering the four countries Norway, USA, Canada, Bangladesh; except Malaysia to analyze how much satisfied the user is among different countries. Malaysia is not considering because this study got only 4% of total participants from Malaysia and this few participants could not enough to analyze the result comparing with these four countries.

The question on the questionnaire has five scales they are *very-satisfied, satisfied, neutral, dissatisfied, and I don't know*. Among them first four scales are considering to analyze the data, excluding the scale *I don't know*. Below the bar chart of Figure 4.5 are representing the result of satisfaction on security from different countries. The aggregate mean value is calculated assigning the weight 1 to 4 in each scale like dissatisfied (1), neutral (2), satisfied (3), very-satisfied (4). The aggregated mean value is using to show the result of satisfaction rate among different countries.

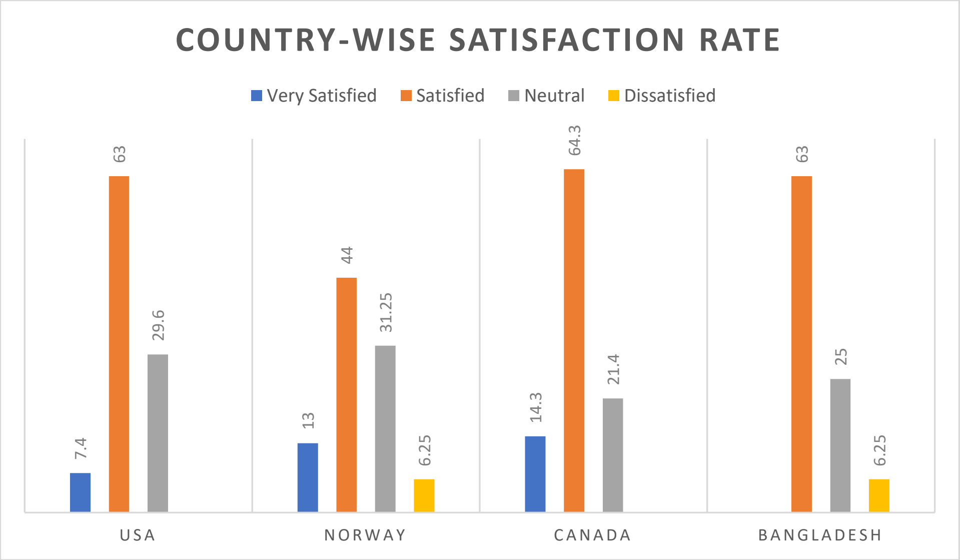


Figure 4.5: Country-wise satisfaction on security

The students of USA has chosen only three scales (i.e. *very-satisfied, satisfied, and neutral*) among the five scales. No students are *dissatisfied* with their e-learning system. Most of the participants are *satisfied* to the LMS they are using, among them, 2 participants are *very-satisfied* and the satisfaction rate for the two participants is 7.4%. One-fourth participant of US are *neutral*. The aggregate mean value of satisfaction in the USA is 2.78.

Norwegian student has chosen all the scale to express their level of satisfaction. Among 16 participants of Norway one has chosen *I don't know*, and it was excluded on the chart. Most of them has chosen *satisfied* and *neutral*. One of them is *dissatisfied* with the LMS. Because of that, the dissatisfaction rate is showing 6.25% for that one participant. Still, a lot of participants was *neutral*. Norwegian students are critical comparing to other countries, this might be a reason to get 31.25% rate in *neutral* and 6.25% rate in *dissatisfied*. The aggregate mean value of Norway is 2.5.

Like USA, the Canadian student has chosen the three scales (i.e *very-satisfied, satisfied*, and *neutral*) to describe their satisfaction on the security in e-learning. Most of the student are satisfied to the LMS, while three respondents are *neutral* and two respondents are *very-satisfied* to the LMS. The aggregated mean value is 2.93.

The Bangladeshi student did not choose the option *very-satisfied*, rather they have chosen *satisfied, neutral, and dissatisfied*. As mentioned before, the e-learning system is not that much developed there in Bangladesh. Only some administrative process is done by the LMS and student has limited options to facilitate their learning process, because of that, the result is like that. Though the chart is showing that, most of the students are *satisfied* to the LMS. Among them one-fourth are *neutral*. Only one participant is *dissatisfied* with the LMS, which makes the dissatisfaction rate 6.25%. The aggregated mean value of Bangladesh is 2.44.

Comparing all the four countries, highest aggregate mean value is 2.93 in Canada, then 2.78 is in the USA, in the third position is 2.5 in Norway, and the lowest aggregate mean value is 2.44 in Bangladesh. It is expected that the mean value of satisfaction would be high in Canada, USA and Norway. However, surprisingly the result is showing that the value is 2.5 which should be at least 2.7. The reason could be the Norwegian students are critical because of that such number of respondent chosen *neutral*, as they have some reason not to choose satisfied as well as not to choose dissatisfied and which cause the value lower than other.

4.2.2 LMS-wise Satisfaction-rate

Here we have considered the LMSs, which are used by most of the participants. From the bar chart of Figure 4.2 it can be seen that *Blackboard, Desire to Learn, It's learning, Moodle* are the LMS which is using by maximum participants. Other LMSs are not considering for this part. The result of LMS-wise satisfaction rate is showing in the bar chart of Figure 4.6. The aggregate mean value is calculated to show the result. Same as above the weight from 1 to 4 is assigned to each scale, in this way dissatisfied (1), neutral (2), satisfied (3), very-satisfied (4).

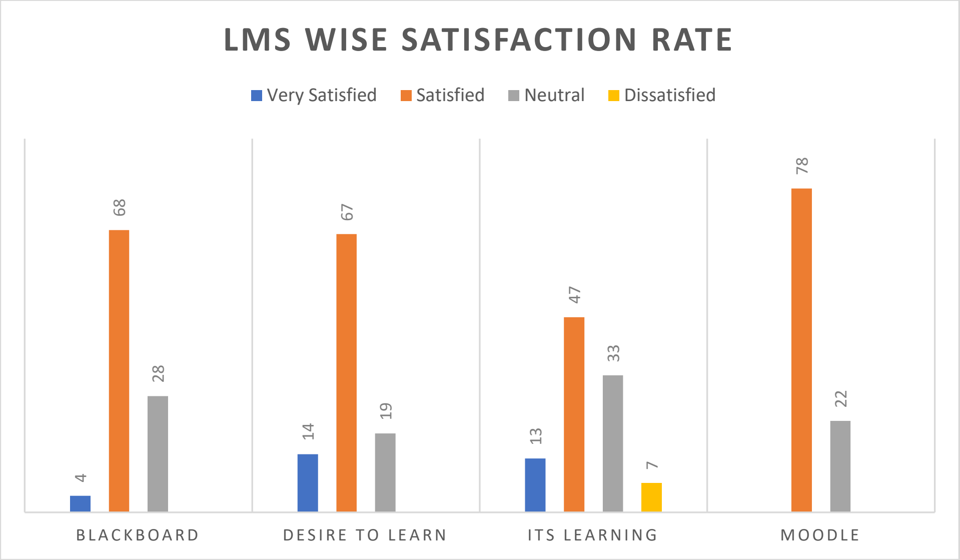


Figure 4.6: LMS-wise satisfaction-rate

The bar chart is showing that among the four LMSs, most of the user are satisfied with the LMS, they are using. About 4% user of Blackboard, 14% user of Desire to learn, and 13% user of It's Learning are *very-satisfied* with the LMS. No one dissatisfied with their LMS except the 7% user of It's Learning. Among the respondents who are using It's learning are mostly Norwegian and most of them are the student of NTNU. The user of It's Learning are facing a different kind of situation, this could be the reason of getting around 33% neutral and 7% dissatisfaction rate. The situation is that from this year NTNU has shifted their LMS, from It's Learning to Blackboard. Some student could think that It's Learning might have some problem because of that this shifting occurs. On the other hand, the student might not like the user interface of It's Learning, and they might face It's Learning is difficult to interpret compared to the Blackboard. Usually, NTNU choose a tender for LMS in each eight years. This time there was an issue occurred with It's Learning and fronter. Because of that issue, It's Learning complained [40], this might create a bad image towards the It's Learning on the mind of students.

The aggregate mean value is 2.95 for Desire to Learn, 2.78 is for Moodle, 2.76 is for Blackboard, and 2.6 is for It's Learning. This result shows that Desire to learn has highest satisfaction value, while the value of Blackboard and Moodle are almost same. However the value for It's learning is little low, because of the described situation.

Secured LMS Ranking 9 respondents have experience of using more than one LMS, and they rate the LMS according to their experiences. Some participants have experience of using *Blackboard* and *Moodle*, therefore they rate only these two; while some other participants have experience of using *Desire to Learn* and *Moodle*, and they rate these two according to their beliefs. The result of this ranking is showing in the Table 4.1.

Table 4.1: Ranking of different LMS

Rank	Blackboard	It's Learning	Moodle	Desire to Learn	Canvas
1	5	2	1		1
2	3		2	2	
3			1		

The table is showing that Blackboard is in rank 1 according to 5 respondents, and in rank 2 according to 3 respondents from all the 9 respondents of the question. As Blackboard is using almost all the selected country, the user of Blackboard is more than all other LMS. This could be a reason to get this kind of ranking for Blackboard. This result shows that *Blackboard* is got high ranking comparing to *Moodle* and *Desire to Learn. It's Learning* is also in rank 1 according to two participants, who have also used *Moodle* and *Blackboard*. That means *It's Learning* considered as the best one comparing with *Moodle* and *Blackboard* by the two participants of Norway.

4.3 Stakeholder's View

Stakeholder's (i.e. students) view in security towards the system are analyzed from the three perspectives, which are named below.

1. From the perspective of *Perceived security, Perceived trust, and Perceived privacy*

2. From the perspective of three basic security components or properties of security which is called *CIA triad (Confidentiality, Integrity, and Availability)*

3. From the perspective of *STRIDE (Spoofing, tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privileges)* threat model.

The answer of participants is analyzed from this three perspective. In the following subsections, the result of these analyses is showing and discussing elaborately.

4.3.1 Stakeholder's View on Perceived Trust

The result of this part is showing that how the students are influenced by *perceived trust*. Because perceived trust influences students behavioral intention to use the e-learning system. When this perception is confirmed, the student's trust towards the system is enhanced. At the same time, they are more likely to use the system. A brief description about *perceived privacy, perceived security, and perceived trust* are given below. Then it is shown that how *perceived privacy, perceived security, and perceived trust* are related. Stakeholder's perceived trust is analyzed from the result of perceived security and perceived privacy. The measure of this perceived trust is adapted from the prior work by Carlos [41]. All items are measured using a five-point Likert scale with anchors from "strongly disagree" to "strongly agree" and weighted them from 1 to 5.

Perceived privacy is the possibility of inappropriate use of collected data about individuals by online company [42]. The growing concern about the security and privacy of personal information and unintended use of it [41]. The user of the online system is reluctant to provide their personal information when the system asks because they are the concern about misuse and interception of their information over the internet. When security and privacy policies are completely disclosed, then the trust of the user will increase and the use of this kind of system will increase [43].

Personal and confidential information can be intercepted and used as fraudulent purpose [41]. ***Perceived security*** defines as a threat that creates a circumstance with the potential to cause economic hardship to data resources or network resources in the form of destruction, modification, denial of service and/ or fraud, abuse, and waste [44]. The e-learning systems do not deal with any financial transaction still they have some confidential data, copyright material, user's personal information, employee or student records etc. To secure these things each system uses some advanced technologies like cryptography, digital signatures, and certificates to protect the user from the risk of fraud, hacking or "phishing". When the e-learning system have implemented security mechanism, the user of the system has started to believe them.

Perceived trust is most important determinant to consider the use of the system and usage of the system [41]. A secure system will get more trust from its user. The trust of the user increases the usage of the system.

Security and privacy have a greater effect on the user's acceptance of e-learning system. Figure 4.7 shows that perceived security and perceived privacy has a positive effect on perceived trust. Trust is particularly influenced by the security, perceived by the stakeholder or user of the system regarding the handling of their private data. Mukherjee and Nath [45] pointed that the privacy and security features of the online service along with shared values are the key antecedents of trust, which in turn positively influences the behavioral intentions of users.

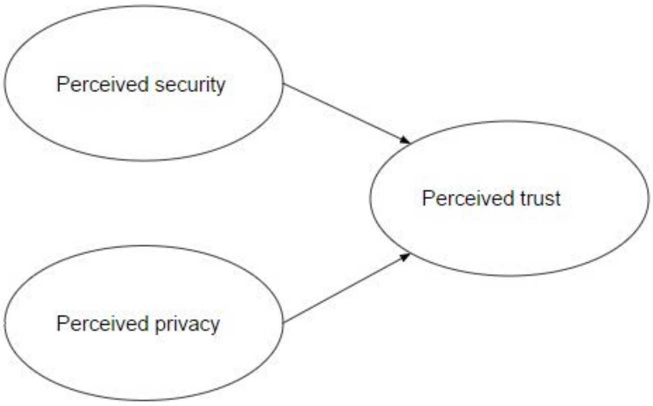


Figure 4.7: Stakeholder's view on *perceived trust*

The following calculation is done by using the software *IBM SPSS Statistics Viewer*, version 19. The reliability of a measure contain no purely random error [46]. The reliability is examined by using composite reliability values and Cronbach's alpha to measure the accuracy of the result. Composite reliability measures the overall reliability of a collection of heterogeneous but similar types of items. Cronbach's alpha measures how well a set of variables measure a single uni-dimensional construct and it ranges from 0 to 1, the higher the value, the more reliable the scale is. The acceptable reliability coefficient is 0.7 yet the lower threshold is sometimes used in the research [41], [47]. The average variance extracted (AVE) measures the amount of variance which is captured by a construct in relation to the variance due to random calculation error [48]. AVE should exceed 0.50 which indicates that the validity of both construct and the individual variable is high.

Table 4.2: AVE, reliability and Cronbach's alpha

	AVE	**Composite reliability**	**Cronbach's alpha**
Perceived Privacy	0.69	0.87	0.83
Perceived Security	0.50	0.80	0.78
Perceived Trust	0.54	0.75	0.73

Table 4.2 shows the average variance extracted (AVE), composite reliability, and Cronbach's alpha of *perceived privacy, perceived security and perceived trust.* In the table, the composite reliability and Cronbach's alpha is above 0.7, which demonstrates adequate construct reliability. The AVE's of the table are above 0.5, confirming that it measures the construct validity of the model.

Table 4.3: Outer loading

Perceived Trust	
The e-learning systems are trustworthy	0.80
The e-learning system has a good reputation to create, manage, and deliver learning content; as well as monitor participants and assess learners	0.85
I do not doubt the honesty of e-learning system	0.67
Perceived Security	
When user make an error, LMS responds with an appropriate error message	0.78
I think the system has sufficient technical capacity to ensure that the data I have sent cannot be modified by third party	0.75
The system has enough security measures to protect my personal and sensitive information	0.76
LMS designed such a way that user cannot easily make serious mistake	0.73
When I have downloaded something from the system, I am sure that I am not downloading any threats for my computer	0.75
Perceived Privacy	
I am concern that the system will use my personal data for other purposes without my authorization	-0.89
The system is recording my personal information without my knowledge like how hard I am working	-0.85
My personal information will be shared with other entities without my authorizations	-0.75

Table 4.3 shows that most factor loadings are above 0.7 except the third item of perceived trust and all the three items of perceived privacy. As the item are construct negatively in perceived trust the value should be negative and it is correct for this study.

The path coefficient is calculated using the theory of Pedhazur [49] and an example using the theory of Pedhazur [50]. Figure 4.8 shows that the path coefficient of *perceived security* and *perceived trust* is 0.50 which is greater than 0.05. The path coefficient of *perceived privacy* and *perceived trust* is -0.75 which is the negative value that means it is not supported by the data. The reason behind this is that the statement for *perceived privacy* in the questionnaire is formed negatively.

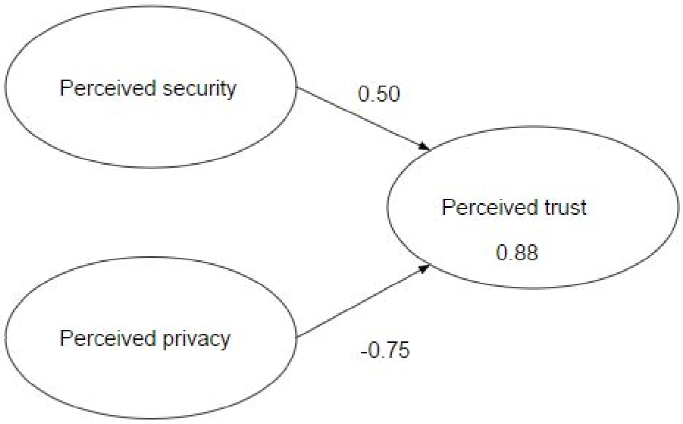


Figure 4.8: Path co-efficient result

The "e" values (roughly error variance) are computed as $\sqrt{(1-R^2)}$ (e.g., $ePerceived-Trust = \sqrt{(1-0.23)} = 0.88$). Thus, examining the model of Figure 4.8 it would be noted that *perceived security* influences the *perceived trust*. The *perceived privacy* is not the determinate of perceived trust.

The reason could be the user of the system are more familiar with the security technology like certificates or encryption keys. Since the security characteristics guarantees of total privacy, the importance of the privacy is relatively lower among the stakeholders. Thus the trust in the e-learning system, jointly in the presence of the security features, drives the decision to provide personal and sensitive information with less discomfort.

4.3.2 Stakeholder's View on Basic Security Property

The basic security property or components of information security are c*onfidentiality, integrity, and availability*, in sort CIA triad [51]. The attack on one of them is an attack on information security and protecting these three components means protecting the assets of a system, (i.e. e-learning system).

Confidentiality *is a property to ensure that information is kept secret and private and do not disclose to unauthorized users. In e-learning system the confidential data are the personal information of user, result or record of student, tracking and monitoring information of user etc.*

To measure the risk in confidentiality of e-learning system, the security risk is analyzed in two angles. One is the *possibilities* of occurring different security issues on different assets of the system, and another one is measuring *harmfulness* of occurring the same security issues to the system. To measure likelihood or possibility three-points Likert scale is chosen from "likely" to "unlikely". Like all other Likert scales "I don't know" is also used for the participant who really does not know what to answer. On the other hand, to measure harmfulness four-points Likert scale is chosen from "very-harmful" to "not harmful". To measure the mean value and aggregate mean value some weights are assigned. For the Likert scale of the likelihood the weights are

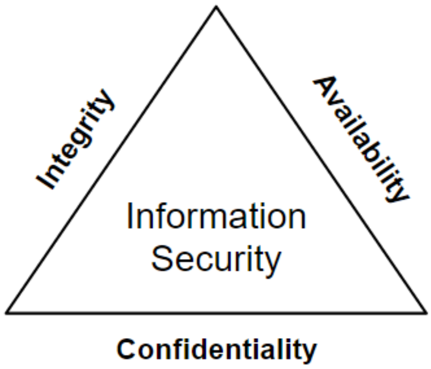


Figure 4.9: CIA triad

3 for “likely”, 2 for “neutral”, and 1 for “unlikely”, and 0 for “I don’t know”. In the same way, for the scale of harmfulness the assigned weights are 4 for “very-harmful”, 3 for “harmful”, 2 for “average harmful”, 1 for “not harmful”, and 0 for “I don’t know”. The considered assets are learning content or lessons, assignments, questions, student records, user account information, admin account information, personal information. Following Table 4.4 is showing the result of this calculation against each asset.

Table 4.4: Mean value of confidentiality of different assets

Confidentiality on assets	**Mean value of likelihood scale**	**Mean value of harmful scale**
E-learning content or lessons	1.43	2.93
Assignment	1.62	3.12
Assessment question	1.45	3.24
Student record	1.62	2.90
User’s account	1.49	3.28
Admin account	1.31	3.42
Personal Information	1.60	3.34
Aggregate Mean	**1.50**	**3.17**

The Table 4.4 shows the mean value of both Likert scale to measure the confidentiality of the different assets of e-learning system. The table shows that the aggregate mean value of likelihood scale is 1.50, which represents that possibility of confidentiality attack on the mentioned assets are from *neutral* to *unlikely*. On the other hand, the aggregate mean value for harmfulness is 3.17, the round value is 3. This value represents that most of the participant thinks the violation of confidentiality in the mentioned assets is *harmful*.

The mean values of both Likert scales are used in the following line graph of Figure 4.10, which helps to represent the mean value more clearly. The lower the line of possibility the more impossible to violate the confidentiality and vice versa. On the other hand, the lower the line of harmfulness, the less harmful the violation is.

The line graph shows that the bottom point of possibility is for the admin account, that means that most of the respondents think that it is not that easy to make available the admin account information. It is obvious, admin account should be more secure, as it is possible to control the whole system from the admin account. Moreover, all kind of data is accessible from the admin account. The participants answered that there is low chance to violate the confidentiality of admin account and they believe that the admin account has enough security to protect the admin account from the violation of confidentiality.

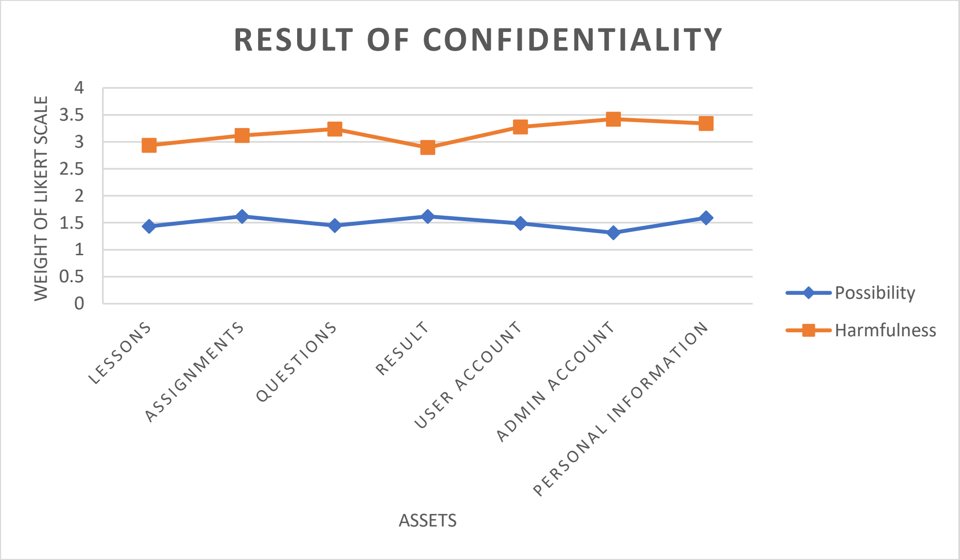


Figure 4.10: Result of confidentiality

The top three points of possibility line are showing for the asset assignments, results or student records and for personal information, and the value is 1.6 (1.6 ≈ 2). This value indicates that the respondents' opinions are likely, which means the respondents think that there is the possibility to violate the confidentiality in these three assets. As well as, the system might not have enough security measures to protect the violation of confidentiality in these assets. The lowest mean value is 1.31 for admin account that value indicates that most of the participants think it is not possible to destroy confidentiality of admin account. All confidential data can be accessed from the admin account. Normally admin account is enough secured so that it can not be easily destroyed. From that believe the participants answered like that.

In the case of the line of harmfulness, the bottom point is showing for student record, and the value is 2.90. This indicates that the respondents think confidentiality attacks on the asset of student record is harmful (i.e. 2.9 ≈ 3), while the mean value for most of the assets is above three. This is showing in bottom position because the number of respondents who think the violation of this assets is not that much harmful. The respondent might not mind if their student record loses the confidentiality, or they might think that this kind of violation is not that much harmful of the e-learning system. The pick in the chart is for the admin account, and the mean value of this asset are 3.42. However the violation of confidentiality in admin account is comparatively more harmful as they are in top position. Because if the system failed to protect the confidentiality of admin account then all kind of confidential data can be accessible from the admin account and it will be really harmful to the stakeholder. Then the purpose of this kind of system will be failed totally and the stakeholder will lose the trust from the system and they will not like to use such system.

Integrity *is the property of protecting the consistency, accuracy, completeness, and trustworthiness of the assets. Protecting data integrity means protecting data from being tempered by an unauthorized user.*

In the Section 3.3.2 it is mentioned that almost same kind of statements are made in the questionnaire to analyze the violation of integrity and the risk is also analyzed from two ways one is the possibility of risk another one is harmfulness of the risks on each asset. From the data of questionnaire the mean value and aggregated mean value is calculated as the same way as above.

Table 4.5: Mean value of integrity of different assets

Integrity on assets	**Mean value of likelihood scale**	**Mean value of harmful scale**
E-learning content or lessons	1.68	3.13
Assignment	1.81	3.01
Assessment question	1.66	3.12
Student record	1.59	3.16
User's account	1.55	3.20
Admin account	1.55	3.08
Forum service	1.62	3.06
Announce service	1.53	3.09
Aggregate Mean	**1.62**	**3.11**

The Table 4.5 is representing the mean value and aggregated mean value of likelihood scale and harmful scale for the integrity of e-learning system. The aggregate mean value is 1.62 ($1.62 \approx 2$) which represents that the possibility of the violation of integrity on the mentioned assets is unlikely. The overall result shows that the participant does not think it is possible to violate the integrity of the system. The aggregate mean value of harmfulness is 3.08 (≈ 3) which indicates that most of the respondent chose harmful from the Likert scale. That means the respondents think that the violation of integrity in these assets is harmful to the system and stakeholders.

The mean values of Table 4.5 are representing in the line chart of Figure 4.11. The line chart is representing two lines one is indicating the possibility another one is indicating the harmfulness as like as the line chart of confidentiality. In the case of the line of possibility, the higher the line is, the higher the possibility of the chance of risk is, on the mentioned assets and vice versa. On the other hand, in the case of the line of harmfulness, the higher the line is, the more harmful the risk is for the e-learning system. The line chart of the possibility scale has a pick for assignment while bottom for announce service. It means that the respondents think the possibility to violate

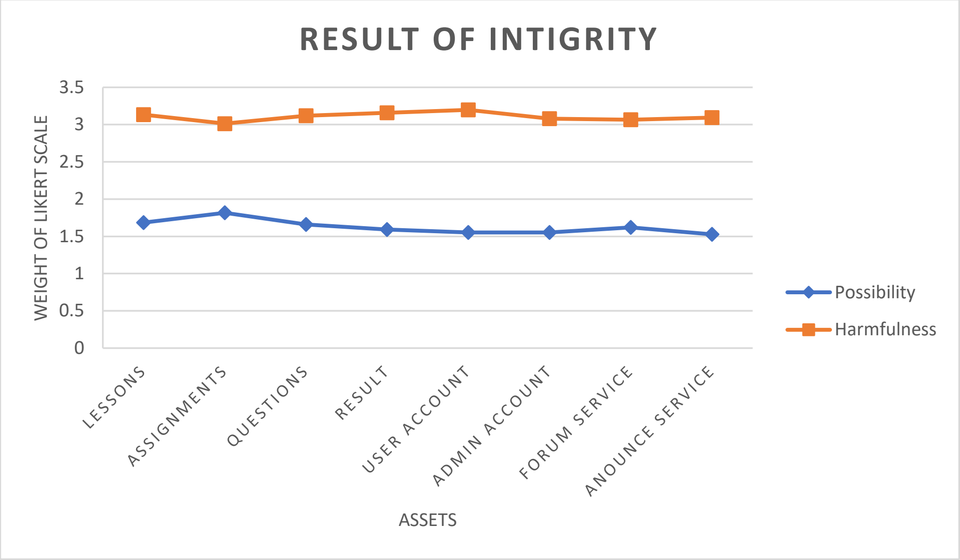


Figure 4.11: Result of integrity

the integrity of assignment is higher compared to the other assets. The violation of integrity in *announce service* is not that possible in the e-learning system. It is because violation of integrity in announce service would not bring that much benefit for the intruder. Although the intruder might somehow manage to violate the integrity of assignment of the system.

All the mean value of harmfulness is above 3, where 3 represents *harmful* from the Likert-scale. The lowest mean value of harmfulness is 3.01 for *assignment* where highest value is 3.20 for *user's account*. Though all the mean values are almost same, still the violation of integrity in assignment is comparatively less harmful. Because it can be recovered by many different ways, for example, the student who has submitted the assignment, has already the file in his device and it can resubmit using another way. The violation of integrity in the user account is slightly more harmful. Violation of integrity in other assets like e-learning content could be recovered by some other ways (i.e. providing sheets etc.) but the violation of integrity in user account could not be recovered so. Security experts should be needed and the whole system might be turned off to recover the whole system. In the middle of the study, the student could not use the system and could not get benefit from it. Moreover, this will be a reason of frustration among the user of the system. Thus violation of integrity in user account will be a great loose for the stakeholder as well as for the system.

Availability *is the property of being accessed and used the system upon demand by an authorized user. As for example, the lessons of the e-learning system are to be made available at the period when the student log in to the system for accessing them.*

To measure the mean value and aggregated mean value of availability of each assets the weight of Likert scale are assigned as follows: always (5), very-frequently (4), sometimes (3), rarely (2), never (1), I don't know (0). After calculation, following Table 4.6 is found.

Table 4.6 shows that the aggregate mean value is 2.08 (≈ 2), which stands for *rarely*. The overall result represents that the participants rarely face availability problem in

Table 4.6: Mean value of availability on different assets

Availability of assets	**Mean value of likert scale**
E-learning content or lessons	2.25
Assignment	2.28
Assessment question	1.97
Student record	1.95
User account	2.01
Email and Messaging	2.11
Forum service	1.80
Announce service	2.04
Aggregate Mean	**2.08**

each asset while using the system. To represent the mean values more clearly a line chart is showing below using the means values of Table 4.6. In the questionnaire 5 point Likert scale used from *always* to *never*.

Figure 4.12 represents a line chart where the lower the line is, the less chance to face the availability problem.

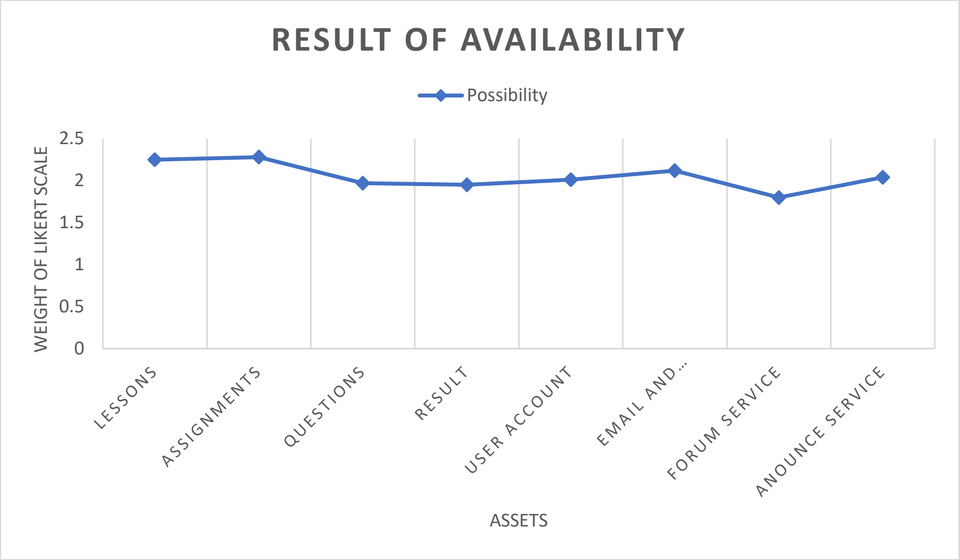


Figure 4.12: Result of availability

The line chart shows that the bottom is pointing for *forum service*. That means the participants face lowest availability problem in that forum service while using the system. Forum service is a service which is not always used by the user and its work is very simple. The student just posts some questions and get some answers for that question. As it work very simply and people do not use the service very often, participant faces less availability problem in that service. All the other point is almost same, yet a little high is for the assignment which is 2.28 (≈ 2) and represents *rarely* from the Likert scale. That means most of the participant rarely faced availability problem in the assignment. They might face problem while submitting the assignment, or while uploading or downloading assignment from the system. This case has also happened that students submit assignment nonetheless do not get the result for that assignment because the responsible teacher does not get the assignment through the system.

From the overall result, it can be noticed that the possibility of violating confidentiality, integrity, and availability is more in the assets *assignment* comparing with other assets. If any attacks happen in the system then the violation of confidentiality and integrity in the *admin account* and *user account* respectively will be more harmful than other assets.

4.3.3 Stakeholder's View Analyzed by STRIDE Threat Model

Microsoft developed the STRIDE model thinking about computer security threats. It is a mnemonic for six categories of security threats. The six categories are [52]:

- Spoofing of user identity,
- Tampering,
- Repudiation,
- Information disclosure (privacy breach or data leak),
- Denial of service (D.o.S),
- Elevation of privilege

Table 4.7 shows the definition of these six categories of STRIDE model. Below each learning assets are analyzed by using STRIDE threat model and combined it with the finding of survey results. Table 4.7 shows that tampering is related with the Integrity, Information disclosure is related with Confidentiality, and Denial of service is related with Availability. The survey results are already discussed by basis of the security components (i.e. integrity, confidentiality, availability). The same things are again showing below for tampering, Information Disclosure, and Denial of Service. The topic about Spoofing, repudiation, and elevation of privilege has discussed by the interviewer which has written briefly in the interview part.

Tampering

Figure 4.13 is showing that among 76 participants how many of them are thinking it is possible to tamper on mentioned assets. The bar chart is showing that the possibility of tampering assignment is highest and the possibility of tampering of user and admin account is lowest. The result is same as integrity. Only the likelihood part is considering in this figure, the harmfulness part is discussed with it yet do not showing in the figure.

Table 4.7: STRIDE threat list [53]

Term	**Definition**	**Security Control**
Spoofing	"Spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage" [52].	Authentication
Tampering	Tampering is illegitimate or non-authorized changes to data or software Data. Tampering involves the malicious modification of data [54].	Integrity
Repudiation	Permitting malicious manipulation by not tracking or recording log of user action [55].	Non-repudiation
Information disclosure	Information disclosure threats involve the exposure of information to unauthorized person	Confidentiality
Denial of service	In this attack misuser try to "make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet" [56].	Availability
Elevation of privilege	"In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system" [54].	Authorization

e-Learning Content Figure 4.13 shows that 15 respondents feel it is possible to manipulate the e-learning contents or lessons by the intruder. If the intruder manipulates the e-learning content then it will be *very-harmful* for the user's of e-learning system, according to 45% respondents. Because, while the student needs to study they could not get the accurate learning material from the system, which can hamper their study, and it will be a reason of frustration among students and teachers.

Assignment Almost 23 of the respondent thinks it is possible to manipulate submitted the assignment and about 32% of the participants think it is very-harmful if manipulation occurs in the submitted assignment. Of course, it is harmful to student. This will be a reason of frustration among the user's of the system. The user will deny to use the function of submitting and getting assignment from the system. As they lost the trust of the system. It is very-harmful for the system. The tampering in the assignment is also very-harmful for the student.

Assessment Question: Most of the respondent does not feel that it is possible to change exam paper before the exam or the exam paper which is going to evaluate. It is because maybe they trust the system so much, or they may have that much confidence that the system has sufficient security which can protect the system from being accessible to the assessment question and being modified by the unauthorized user. Almost 38% student thinks it is very-harmful and 42% student think it is harmful if the assessment question is modified by any intruder. It is really very-harmful, because if the assessment question is modified by the unauthorized user before the exam, then it will stressful for the subject teacher as well as for the student. Because they will come to exam hall being fully prepared for the exam, then they may get

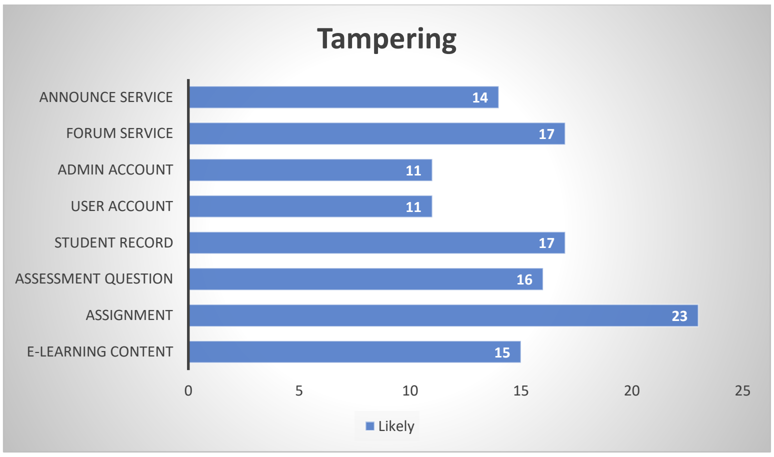


Figure 4.13: Tampering in e-learning system

the modified question or before that, the teacher can be noticed about the modified question. Then sometimes of the exam will be wasted to re-setup the real question. Another scenario can happen if the subject teacher does not notice that the exam paper has modified, then the student will answer on wrong question paper, which could be out of syllabus, then the educational institution may have re-arrange another exam for the student because of wrong question paper. That is frustrating for the students and other users relate to the exam.

Student Record 17 respondents think it is possible to manipulate the student records where 42% of the respondents think it not possible. Most of them think it is not possible to manipulate the student records. It means most of them trust the e-learning system. Still, half of them thinks it is possible to manipulate, it is because maybe they think no system is 100% secure. Many new ways can find out by the hackers to hack the system. If the student record is manipulated by any intruder than 49% of the respondents think it is very-harmful, 33% think harmful. The student record represents their performance as a student in the educational institution. Hence it should be accurate as it judges a student how good he is as a student in his subject. After graduating from university they will apply for the job. If they came out from the university with manipulated result then this record will represent them wrongly and this will be very-harmful to their future career.

User Account 11 respondents think it is possible to control the user account by the intruder. From this result, we can see that most of the student believe that intruder can not get control of their account of the e-learning system. Get control of user account is very-harmful according to 51% respondents, harmful according to 30% respondents. Almost half of the total respondents believe it will be harmful if any intruder gets control of their account. It is harmful because the lesson of the different course and a lot of important notice, and other stuff are stored in students account. However if intruder temper the stuff then the student will not get benefit from it. Moreover, in the middle of the study, they have to collect all the necessary things from the department manually.

Admin Account In the case of the admin account, the same number of the respondent (i.e. 11) think it is possible to get control of the admin account. Most of the respondent were neutral in their opinion because the respondents are not security expert and they don't have enough knowledge. On the other hand, they might have some reason for both possibility and impossibility and because of that they choose neutral. Very few of the respondent thinks admin account could be controlled by the intruder, nonetheless most of the respondent do not believe it is possible. Obviously, admin account of any system should be more secure, because it can control the whole system. On the other hand, get control of admin account is very-harmful according to 46% respondents, harmful according to 32% respondents. Because it can modify or destroy all the data, even the main user can lose his own account. Tampering in some user accounts can affect one or few users, however getting control of admin account is more dangerous. Because whole system can be destroyed or modified by the intruder if admin account hacked, every user will be affected by it.

Forum Service Almost 22% respondents think it is possible to manipulate posted the question in forum service, again 37% respondents thinks it is not possible. The student post questions in the forum service related to their lesson or exam syllabus or if they do not get anything from the syllabus or lesson. The reply of that posted question can be given by the subject teacher, or teaching assistant, or by another classmate. If the posted question or posted information changed by intruder then the other student or teacher who will see the modified post they will get wrong information which is useless for the student sometimes wrong information might lead them to the wrong direction. The post might be about the exam of tomorrow, if intruder changes the subject or topic of the posted answer then there will be no time to recover the thing and student will go to exam hall with wrong information which might affect their answer of exam as well as result. In that case manipulating posted question of the forum, service is harmful.

Announce Service 14 respondent thinks it is possible to manipulate the information of announce service. Changing old information will not cause any problem. Nonetheless changing up-coming information might cause some problem for example there is some deadline for registering 'Thesis'. The announce service reminds it to the students few days ago. However, if someone change the actual date of deadline than it will make some problem. Still it is possible to solve manually. After the deadline of registration has been passed, the student would go to the office and then the responsible person would help them to register the thesis in the system.

The result shows that the participants think chance of tampering is high in the assets 'assignment', and low in the asset 'admin account' and 'user account'.

Information Disclosure

Figure 4.14 shows among 76 participants how many of them think the system has threats involves with the exposure of information to unauthorized person in different assets.

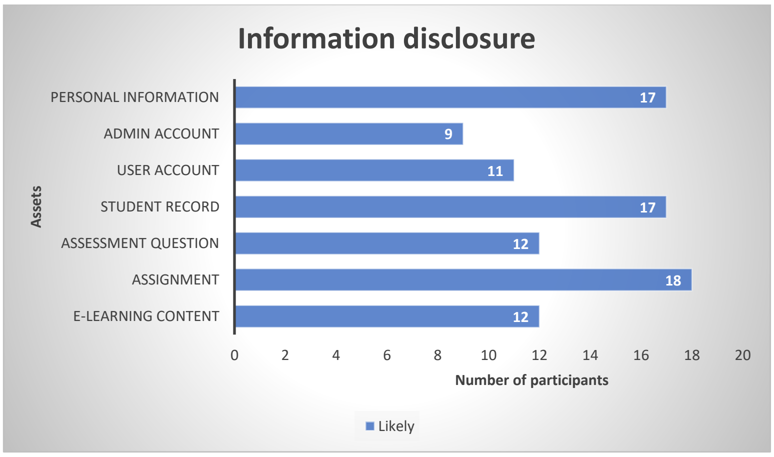


Figure 4.14: Information disclosure in e-learning system

e-Learning Content It is possible of information disclosure in e-learning content answered by about 16% of the respondents. The respondents think it harmful to get access to the e-learning content by an unauthorized user. It is because their may have chance to destroy all the content or modify the content, which can be very-harmful for the student.

Assignment 18 respondent thinks information disclosure is possible in the asset assignment, while approximately 41% of the them do not think it is possible. It is because e-learning system has secure log-in system, hence unauthorized user could not log-in to student account. If they fail to log-in to the student account then it is not possible to submit assignment on behalf of others. Yet if one user allow another to see his assignment or submit assignment on behalf of him then it is possible. If the system has any security hole which enables the student to see each others assignment than it will be harmful for the education system. Student will not get actual credit for his work and the student who copied the assignment from other students will not learn anything.

Assessment Question 17 respondents from 76 respondents think information disclosure is possible in assessment question. No system is 100% secure, from this angle it is always possible to break any system. Thus it is not impossible to get the assessment question which is stored in the e-learning system by intruder. If intruder make the question available before exam then it will be harmful for the education process. If there is no time to make another question than student may have to sit for exam in another day. But if the subject teacher or instructor have no knowledge about this information disclosure than the student who got the question will perform better comparing to other student, which is also not right for the educational process.

Student Record Information disclosure in student record is also possible answered by 17 student. The respondents might not believe in the security of the system or they might think there is always some intruder who want to destroy the system. Sometimes getting access to the student record may be beneficial for the intruder. Thus the intruder are trying to find out new ways to break the system. Information disclosure in student record is not very-harmful nonetheless it is not right. Moreover student do not want to share their result to other. It will destroy their privacy.

User Account 11 respondents think information disclosure is possible in user account, though most of them do not think it is possible. There is some password policy for each institution, where there is a rule for each password (i.e. combination of capital and small letter, with digits and special case letter. The password limit is minimum 8 character). The purpose of this rule is to ensure a not guessable password, or to protect the system from the attack like, dictionary attack. In the password policy there may have another kind of rule like password must be changed after each 6 months. This policy is made to make the system secure. It is also possible if intruder find out a way to hack user's account.

Admin Account only 9 participants among 76 participants think information disclosure is possible in admin account. If we compare the result of 'admin account' with the result of 'user-account' then we see that the respondent believe admin account is more secure than user account. Admin account should be enough secured of any system. Because this is the account which has control on the whole system, including the information of other accounts, and other related data. Thus most of the student believe that the system has enough security from the unauthorized access to admin account.

Personal Information Information disclosure of personal information is possible, answered by 17 participants. Personal information is like SSN (Social Security Number), Student ID, log-in credential etc. This personal information is beneficial for the intruder. They can use it to get access to the system as an authorized user. They can miss-use the SSN, or send the user some harmful mail, by which different kind of attack is possible to the system.

The result of information disclosure shows that the respondents believe that the chance of information disclosure is higher in the asset 'assignment' and lower in the asset 'admin account'.

Denial of Service

Figure 4.15 shows the result that among 76 participants how many of them faced denial of service (DOS) in the mentioned assets, which are described below.

e-Learning Content The learning resources must be available when the user need them. Among 76 participants, 2 of them always, and 6 of them very frequently face availability problem when they want to get access to the e-learning content. The reason behind this might be, at that moment either learning resources or the e-learning system is not available because of some network or server issues. However the result shows that most of them do not face the problem.

Assignment While uploading or downloading an assignment 2 participant always, and 9 participant face very frequently denial of service. This result is also showing that most of them do not often face the problem of the assignment. However the

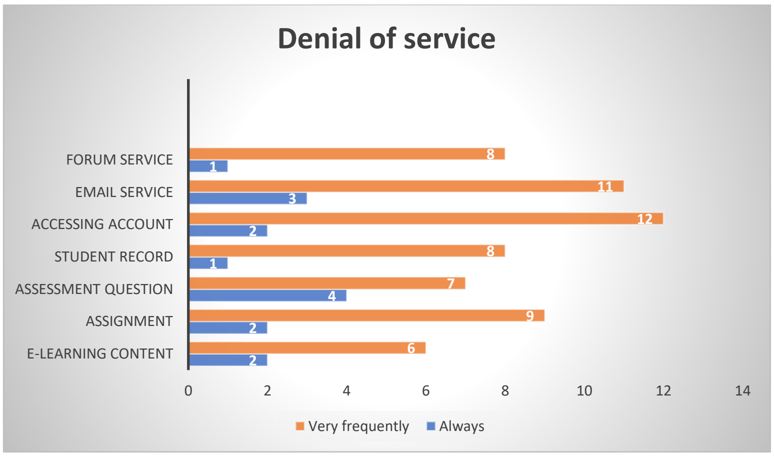


Figure 4.15: DOS in e-learning system

participant who faces the problem either there is an issue with the e-learning system or the network or the server. Another question was asked to the participant that, "have they ever faced the problem that they submit an assignment to the system and the system denied it?". No one answered always and very frequently yet 16% answered occasionally they faced the problem. This issue is related to the e-learning system.

Assessment Question Among 76 participants 4 participants always, and 7 participants very frequently face denial of service problem while they have to open the question from the system at the starting of the exam. That means their system has some problem of opening the question paper at the starting of the exam. At the starting time of the exam, it is allowed to all of the students to open the question paper. If at that moment student fails to open the exam paper then, this problem will kill some of their time from that limited time for the exam.

Student Record The result shows that 1 participant always, and 8 participants very frequently face denial of service problem when they try to access their student record. It may happen when e-learning system is not available, or there is some network issue, or student record is not available at that moment.

Account The result shows that 2 participants always faced, and 12 participants face very frequently denial of service problem while they want to access their account. Another problem is that after logged in, the system could be denied to show the account information which has been faced always by 3% respondents, very frequently by 13% respondents. Thus the e-learning system could have this kind of availability problem it may happen because of DoS attack, network connection problem, unavailability of e-learning system etc.

Forum Service Among 76 participants 1 is always and 8 participant is very frequently faced denial of service to post something in the forum of e-learning service. This could happen because of unavailability of e-learning system, network connection problem, or unavailability of forum service.

Figure 4.15 shows slightly different result than the result of availability. The reason is that, here two point of scale (i.e. very-frequent and always) is taken to show the result. The overall result of DoS shows that student face denial of service mostly while they wanted to open the assessment question in e-exam. The rate of facing the denial of service is lower in the asset 'forum service', 'student record', and 'e-learning content'.

Elevation of Privilege

Authorization is an important part, to maintain the security of a system. If the system has security holes and the unprivileged user gains privileged access then all kind of possible damage can happen to the system.

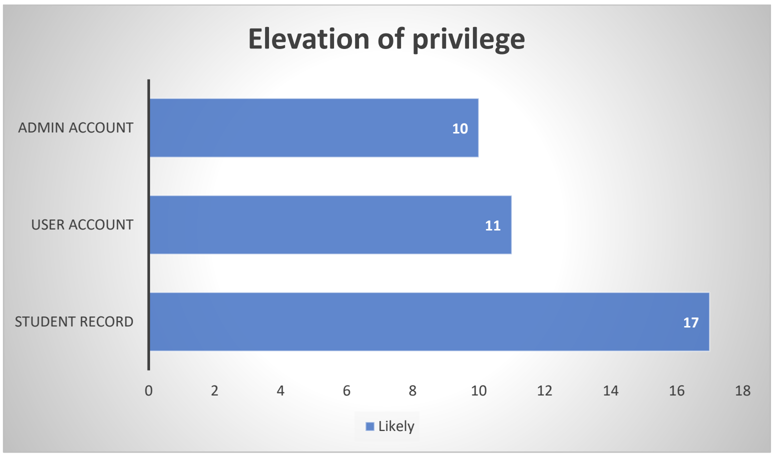


Figure 4.16: Elevation of privilege in e-learning system

Figure 4.16 shows unprivileged access and control is possible in admin account by 10 participants, in the user account by 11 participants, in student record by 17 participants. A right person controls the right account is most important to maintain the security. For example, the unprivileged user gets privileged access to the student record, and he might use the advantage for his own benefit by changing the whole record or delete everything from the system to destroy the fame of the university.

The overall result using STRIDE threat model is same as the result of CIA triad. The result shows that tampering and information disclosure is possible in *assignment*, and the respondents faced denial of service mostly while accessing their user account. It is obvious, as shown in table 4.7 tampering is the violation of integrity, information disclosure is the violation of confidentiality, and denial of service is the violation of availability. In the questionnaire, there is no question made for spoofing, repudiation, and elevation of privilege. As the questionnaire is made for the general student, and technical term is avoided there, because of that this three topics is not included in the questionnaire. Still, the questionnaire has the question about authentication and authorization, which became the part of the asset *user account* and *admin account* and discussed in the tampering and information disclosure section.

4.4 Encountered Security Issues

This aim of this section is to find out the encountered security issue of e-learning system. Encountered security means here that, if the user of the system have ever experienced any security threats or issues, or have they ever heard about that kind of issues from anyone, have they ever experienced any un-permitted sharing of copyright materials etc. Below some experienced security threats or issues encountered by the participants are discussed.

In the survey, some participants shared their experiences on the security issues of their LMS, either they have faced or they have heard from someone about the issues. One respondent said that "Students in Norway got access to other students *it's learning* page last week". That means It's learning has the possibility to access anoother user account. The intruder who has accessed other students account, might know the log-in credential of that student, or he has accessed through the public computer where the log-in information is stored by default. A hacker can use a lot of ways to access or hack user account, like Cross Site Scripting (XSS), Insecure Direct Object References etc. Another user of It's learning and Fronter commented that it has the possibility to send false messages. The author is also a user of this LMS, and also experienced getting false messages and spam. Another student of It's learning comments that he has submitted an assignment and the system of the subject teacher denied it. Therefore he sends a screenshot from his system that he actually submitted the assignment. One user of Google Classroom commented that they have difficulty in accessing their user account. Another user of Google Classroom commented that some hacking occurs in that LMS. A blackboard user commented that other person also received the email when he sends an email to a person. 'Desire to learn' user experienced that students are giving exam together which is not allowed. Moodle and Desire to learn user experienced the error in their grading system.

Among the participants, about 21% experienced un-permitted sharing of copyright materials. About 13% respondents experienced wrong or false information sometimes by the system.

4.5 Result from Interview

This section will describe the findings from the different interviews conducted for this study. The interview questions are showing in Appendix B. In the Section 3.4.4 it is described that how coding is done from the transcription of the conducted interview. In the last part of the section 3.4.4 a Table 3.2 is made from the raw interview data and coding. The next part of the post work of interview is making the example quotation table from that table. The table is not discussed in the previous chapter as they are the part of the result of the interview. The tables are from Table 4.8 to Table 4.13, and each table has three column. The first column is representing the primary theme, the second column is representing sub-theme which is the primary theme, and the third column is showing the main quotation from the interview related to the theme. The following section is presenting the tables and describing the result elaborately.

4.5.1 Key Assets of the e-Learning System

All the informant told about the key assets of the e-learning system, and the mentioned key assets are almost same. The assets like the assignment, personal information's are not related to the academic integrity, and grading of test and answer of the test are the assets which are related to the academic integrity. Key assets of e-learning system are discussed below from the interviews.

Student Record

There are two types of test results one is part of end grade and another one lets a student give access to the final exam. Blackboard includes only the test which will approve a student for the final exam.

"Student might want to fiddle with the result of this test because it affects whether they will take part in the final exam or not. Because if somebody is able to log-in with the privileges, they can change the test results and reverse the result of bad tests, so that they can get access to the final exam". - Informant X

NTNU has decided not to use any graded test in the current installation of Blackboard. Blackboard has another system for the test with natural grading, which is part of end grading. The official reason for that is security. NTNU wants to have one system for all task and do not want to spread the exam on partly in Blackboard and partly in another system.

All the informants think that student record or grade is an important asset. Therefore, it should not be changed by any intruder and it should be set by the right person.

Student works

Student works for example assignment, thesis, term paper or answer of the examination etc., are usually submitted by the student in the e-learning system which is another key assets of the system said all the informant, and it should be protected. This key asset is related to the academic integrity.

"Student's work should not be copied or lift upon by others. In some circumstances, there are some assignments and articles made publicly available on purpose, but that's another thing. But if they are supposed to be kept secret from students for other reasons like for plagiarism, then it should be cared for about." - Informant Z

So preventing people from seeing student's work is important because there is a chance of copy the work and the student will not get their credit and sometimes they might lose marks for their work which they really deserve.

Personal Information

Personal information is the most important key assets of the system because losing personal information means losing everything by giving access to his account to the intruder. If the intruder gets access to the admin account then the loss is much bigger because in that way he can get access to the other assets like student record, student's work etc and able to destroy them.

Normally e-learning system does not have that much sensitive information. Yet it has some personal information which can be useful for the intruder. On the other hand, in some cases it is better to act anonymously in this system or process for example

Table 4.8: Quotation from interview regarding on the key assets of the e-learning system

Theme	Sub-theme	Participants Quotations
Key Assets	Student record	"Grading of test relate to academic integrity. No one wants to leak their student record or grades. Intruder may want to change his grade as it might improve his profile." – Informant X "The grade should be set by correct people" - Informant Y
	Students works	"No one wants to be leaked their work before the date." – Informant X "It is important to prevent people from seeing examination or answer because there might have some information which should not accessible by supervisor or sensor." – Informant Y "Student's work not being copied or lift upon by others. In some circumstances, there are assignments and articles made publicly available on purpose, but that's another thing. But if they are supposed to be kept secret from another student for other reasons like for plagiarism, then it should be cared for." - Informant Z
	Personal Information	"By stealing personal information an intruder can act as an authorized user, and can do anything that a student can do. Of course, the intruder will use this privileges from bad intention" – Informant X "Exam system has some personal and company sensitive information which should not be accessed by the supervisor or sensor" - Informant Y

forum is used for a different kind of educational discussion, in some cases, the student wants to share some honest opinion anonymously. In the examination, the answer of the student is anonymous because containing personal information can affect in the marks of students.

"In examination system, there might be information either about yourself or about the company you are working with which is not supposed to be accessible by other supervisor or sensor. Thus exam system has personal information and company sensitive information." - Informant Y

The e-learning system should keep the personal information securely.

Some Other Assets

There are some other assets which need to be protected.

"You also have integration point that we do not want to access by anyone. We need to protect all the end points or all the solutions, the system itself, and the user account, hardware or user computer." - Informant Y

4.5.2 Security Issues related to the System

All the informants think that this kind of system does not really have a lot of security threats, though it is possible to attack such system. The effect of destroying it will not be really big. Still, there may have some reasons to destroy the system like, exposing teacher, stealing user account information, making information available or cheating in the examination etc. The informant has some previous experiences of security attacks and they are resolved now.

Possible Threats

There may have some possible threats in the system though they do not happen yet in their system.

"Unauthorized access is the main threats – depends on password and user affiliation. The best way to protect authorization is using Feide." - Informant Z

Some other possible threats of the system are DOS (Denial of Service), hacking, identity theft, making information available to the system, change the grades of the student etc. If any one gets unauthorized access to the system then he can do any of this attack.

An interviewee thinks there might have some other vulnerabilities, which have discovered by the user of the system. As the user do not report the issues yet, they do not know about the current threats to the system. Moreover, they did not face any direct attack or identity theft attack.

Experienced Attacks

The informant has some experience of security attacks, and how much harm in the system happened for the attack are discussed here.

One phishing attack happened in Blackboard in last December. Intruder sent a lots of mail, stated that the user needs to login a page to update their Blackboard password. That was just a normal phishing attack. In this kind of attack it is possible to send an alert email to all the user not to open the vulnerable email, and then no one will be harmed by it.

"INSPERA assessment", sort of browser software which locks down the examiner's computer, that makes unable to use the computer for other things that deal with the exam. However, this software was fooled by a couple of master's thesis students. They fooled the software, by building their own version of the software (probably putting there some loopholes) and run that instead. This has been removed by using desktop session. That is kind of a way, where the student could make fool the software and cheat during the exam. However, in the examination hall, there are people, who are looking what are examiner doing. If one can technically fool the system, he can still be caught and throw out from the university.

FS (Felles Studentsystem - a common administrative system) is a software where all the courses and student are fit into it. It is a big administrative process, where everything related to student's grades, course etc, are integrated there. This system integrated with exam system. The exam system persists on several services like Google Analytics. Limited direct control of what kind of third parties they included into their solution. By using third parties it is possible to get access to personal information of user like IP address. Sometimes it needs to ask to remove some third parties because it could be vulnerable to identity theft, for instance, one can steal teacher's digital identity and set grades. Thus, the system should be aware of this threats. This kind of third party issues has been experienced by them. Then they asked some of the

Table 4.9: Example quotation from the interview regarding on security issues of the e-learning system

Theme	Sub-theme	Participants Quotations
Security Issues of the system	Possible threats	"Exposing teacher or destroying the creativity of the teacher, stealing user's account information, cheating in the exam- can be a reason to attack such system" – Informant X "DDOS, hacking, identity theft, making information available, change the grades of student could be possible threats" – Informant Y "Unauthorized access is the main threats of such system" – Informant Z "Web conferencing on lecture webinar- possibility to make a recording of the session. After recording they can make it available without permission, which will violate the right to the material." - Informant Z
	Experienced issues and their solution	"A normal phishing attack was happened by someone who sent a lot of mail to the Blackboard user by stating that they need to update their Blackboard password" – Informant X "Some master's student tried and succeeded to fool the software 'INSPERA assessment' by making their own version of the software, and this can be removed by desktop session." – Informant Y "Some third parties were vulnerable to identity theft in FS (Felles Studentsystem), so it needs to request to remove the third parties." – Informant Y "7-8 years ago, there were some downloadable video session cookies. By these cookies, it was possible to log in the system as a teacher. After being detected the vulnerability was eliminated. The thing is that if the teacher log out and turn off their machine afterward that is not a problem, but if the teacher keeps it running and go home, then that is a vulnerability." - Informant Z
	Encountered problem	"The problem is more related to the trade-off between functionality and security. The more tighten the security the less functionality the system have." - Informant X
	Challenging security issues	"As Blackboard is a patchwork of software it is difficult to reorganize from bottom-up to fix security problems. Maintenance of security and stability is very difficult as the code is just a bunch of historical trade-offs." - Informant X

providers to remove the vulnerable third parties and make some contractual agreement about providing data to third parties. By this way, the problem was solved.

“Good evaluation of our provider and good legal contract hopefully will prevent major risk.” - Informant Y

“NTNU owns its own data. When they have an agreement with third parties, they need to go for a contractual agreement about their sort of use and manage their administrative data. Many third parties may involve. This agreement also needs to involve third parties as well like a legal tool of involving data.” - Informant Y

7-8 years ago, another security issues were found where the intruder can get access to the system as a teacher using some download-able video session cookies. After being detected the vulnerability was eliminated.

“The thing is that if the teacher log out and turn off their machine afterward that is not a problem, but if the teacher keeps it running and go home, then that is a vulnerability.” - Informant Z

Trade-off between Functionality and Security

In Blackboard, it is possible to load modules to get extended functionality. To load the functionality the LMS need to enable some privileges. One teacher may want to load a certain privilege which may helpful for his course, however the system operator may find some problem in security (i.e. this will create a big hole in the security of the system) and stability to load the privilege and refuse to load it.

“The more you tighten the security, the less functionality you have.” - Informant X

This problem can be solved by convincing, for example, the teacher may convince the provider that he needs this functionality to get the privilege. But if the provider finds it is not possible, because they have, for example, 40 thousand customers who may face another type of security problem if they give that privilege to the teacher.

Challenges

Blackboard is a patchwork of functionality. It does not sell a well-designed software; they sell a patchwork of a different kind of software. It is difficult to re-organized from the bottom-up to fix some security problem. If they need to correct something, they would never be able to go the bottom and re-design the system from the bottom to up. Blackboard has tried to re-design from bottom-up, but it is too big and too slow with respect to development speed. On the other hand, they must support current installation base and add more functionalities, as everyone is screaming for more functionalities. Hence, they ended up with a very complex and diverging base of code. Therefore, maintenance of security and stability is very difficult as the code is just a bunch of historical tradeoffs. Blackboard have a lot of functionality, it is a kind of stability, which is also a problem.

4.5.3 Cheating in the e-Exam

Cheating is writing or saying something that is correct without having done the process of learning. People are cheating in the exam for ages, it’s nothing new.

“The more traditional way you have, the more cheating you get.” - Informant X

There are several possibilities of cheating during the exam or after the exam e.g. change of grade. To improve the grade in the exam some student always tries to cheat on the exam. In the e-examination how the students manage to cheat, what are measures taken against it, is discussed here.

Structure Questions such a way which Makes the Student Difficult to Cheat

"Cheating is much more related to how you form the question, rather than existing security threats in the question." - Informant X

The potential of cheating is depending on the structure of questions. If a question has a definite answer than it is easy to cheat. If a question is made based on the understanding of the topic, then it will be difficult to cheat. Same as open book exam, if a student has all the books and he does not know about the topic then it will not help him to write the answer because the student must know the fact to give a good exam.

If we divide a programming exam into two types. One type has a programming routine (that does this or that), which gets some parameter, and then ask what will it print out. Another type of test can be based on the understanding of the code, what is happening there? This type of question is more difficult because the student should try to understand the code in this kind of question. The student might think if they have editor and compiler to solve the problem, then he could do better. However, most them will not because they must fix the bugs and errors of the code first to run the code and get the result.

Cheating Experience

The informant share their experience of cheating in the example. In last autumn, in a programming examination, two students went for pause at the same time. When they get back they switched their position and fixed up each other's work and then went for pause again to switch back. That's a type of cheating.

There are many ways of cheating and impossible to eliminate them like some student may use the ear piece or bring notes in the pockets etc. The student cannot do this kind of cheating in large scale and cannot give a lot of effort in doing it. Most of the exams are such that, a student cannot put a lot of effort in it.

In LMS, if a loophole was found which enables students to cheat, and a lot of students can cheat quickly by it, then the academic integrity of the whole system will lose. Cheating of one student is bad, however cheating of all student is fundamentally bad. The potential for that is much bigger in a computerized system than the paper-based system. The scalability of the cheating problem is much bigger for the computerized system, then paper based system and that is much worst for the institution too.

Non-technical solution vs Technical solution

The non-technical issues are as important as technical issues. If one student sits in the examination hall for another student, the examination system may have a good technical solution but if the people on the exam area does not see who the student is, it does not help. A good technical solution does not work if the student has a copy of note in his pocket or in his bag pack, or phone in the toilet. Thus, the technical

Table 4.10: Example quotation from the interview regarding the cheating in the e-exam

Theme	Sub-theme	Participants Quotations
Cheating in e-exam	Structuring question such a way which makes cheating difficult	“If a question has a definite answer than it is easy to cheat. But if a question is made, based on understanding of the topic than it will be difficult to cheat.” - Informant X
	Cheating experience	“In a programming examination of last autumn, two students went for pause at the same time, but when they get back they switched their position. Then they fixed up each other’s work and possibly they went for pause again to switch back. That’s a type of cheating.” - Informant X
	Possible ways of cheating	“Possible ways of cheating in e-exam could be using the ear piece, note in the pocket, using loop-hole of the e-exam system.” - Informant X “Information system exposing like knowingly or purposely sharing their exam, which should not be sharing with and people providing access to other people that should not be happened.” – Informant Y
	Non-technical and technical solutions	“Technical solution is not the only side to prevent cheating in the exam, for example, having notes in the pocket or in the bag pack, phone in the toilet, it does not help with the technical solution. Monitoring during the exam, and if it is found that a student is cheating to stop the student from cheating manually rather than making it impossible to break the system because that could be extremely expensive.” - Informant Y
	Measures	“We could disallow all the wireless network that are in the area. We prevent the student using their phone as a hotspot that could have potential to communicating with another side through some other network. Face recognition system to make sure the correct student is giving the exam. We could record the screen to see what they do all the time. There is billion of the solution to prevent the cheating. A lot of issues, which could have exposed to for example knowingly or purposely sharing their exam, which should not be sharing with. People providing access to other people that should not be happened.” - Informant Y

solution is not the only side of it. It is not always certain that technical solution is the best one.

During monitoring in the examination hall, if it is found that a student is cheating, to stop the student from cheating manually rather than making it impossible to break the system. Because that could be extremely expensive. Thus, may be log-in and monitoring and sort of working around in the examination hall is equally viable. There is always a loop-hole. If it is technical, it is going to break. The security expert have to prepare for it, when it breaks should try to prevent it, try to measure it, that could deal the expose which already have.

"One debate we have there is whether we should allow people to use their own client or own PC, whether we should have NTNU owned client. Of course, we have a lot of control over the NTNU owned client, but it cost a lot of money to buy a lot of computers. So maybe it's better and cheaper for the university to accept that it's technically few more possibilities to cheat but we could take other measures, that hopefully stop the student from cheating."

So, it questions of what kind of risk level the institutions are willing to accept and how much money they are willing to spend on solving them. They could also set up firewall solution, or could make sure it is impossible to communicate, could have the log-in solution, that monitors the traffic that is in place. There are many measures to prevent from cheating. The consequence of caught cheating- expel the student, disallow from all universities at least for a year.

Measures

To avoid cheating in the exam, the informant thinks it is necessary to prevent people from talking to each other, having access to the information, which is not supposed to have, or having another people doing examination from another place.

The institution could disallow all the wireless network that are in the area, could prevent the student using their phone as a hotspot that could have potential to communicating with other side through some other network, could use face recognition system to make sure the correct student is giving the exam, could record the screen to see what they do all the time. There is billion of the solution to prevent the cheating.

A lot of issues, which could have exposed to for example knowingly or purposely sharing their exam, which should not be sharing with. Another information system exposing is people providing access to other people that should not be happened.

4.5.4 Shifting from Modern e-Learning Ecosystem or Cloud-architecture

The informants' opinion about the shifting from traditional e-learning system to modern e-learning ecosystem or cloud architecture are discussed here.

LMS is a total e-learning experience, which has an interface and everything meets into this interface. For example, Blackboard, It's learning. Monolithic LMS is used in the different institution, which is a mandatory way of using electronic teaching. Blackboard and It's learning are monolithic in a sense that it does not connect well with other pieces of software. In modern e-learning ecosystem, it is possible to use any tool in order to full-fill the necessity of the user. This external tool can talk together in this e-learning ecosystem.

Table 4.11: Example quotation from the interview regarding the shifting from monolithic to modern e-learning system

Theme	Sub-theme	Participants Quotations
Shifting from monolithic to modern e-learning ecosystem or cloud-architecture	General opinion about this shifting	“Monolithic LMS is used in the different institution, which is kind of a mandatory way of using electronic teaching. For instance, Blackboard and It’s learning are monolithic in a sense that it does not connect well with other pieces of external software. In modern e-learning eco-system, it is possible to use any tool per necessity of user. This external tool can talk together in this e-learning eco-system. But the LMS does not have this functionality for doing that” - Informant X “In e-learning ecosystem or cloud-based system, there is limited control over the infrastructure, the configuration. To have good configuration and good change management they must rely on third parties. On the other hand, the monolithic system is expensive and might not have the expertise that some other partied may have. It is easier to do something secure in large scale because you could use more effort and more resources on securing the service, rather than spreading out a lot of effort on a lot of different places. When you do not have the full control in the system, you could sometimes get longer to get support. For example, need to turn off the system, or change something which could expose the security risk.” – Informant Y
	Problems of the monolithic system	“In e-learning ecosystem the teacher may want to use whatever tools most relevant to the subject, but in LMS, the teachers are constructed to whatever tools are made available for the teacher to teach the subject.” - Informant X “The teachers do not want to explore the net for different tools, rather using the tools of LMS provided by the university. Which is end up instead of providing the best teacher with the best tool, they are providing the best teacher with the average tool and force the teacher to use average quality resources. That is a problem because it reduces the motivation of excellent teaching” – Informant X “If a teacher wants any special kind of functionality which is not present in the system, but available in the net, then he can use it but cannot connect the functionality in the system. This could create a lot of problems” - Informant X
	Advantage of monolithic system	“Simplifies a lot of administrative processes like the moment a student register a course, the course automatically show in his user account” - Informant X

Problem of Monolithic System

Some problems of the monolithic system from the informant's knowledge are described below.

As we know the monolithic system is a bunch of a different kind of software or functionality. Among those, some may not provide that much facility like other existing tools available in the net. For example, Blackboard has a simple forum software for discussion, which is badly written, and does not have the complexity of teaching process (i.e. does not have the question answer for the teacher, teaching assistant, and student etc.). While in the internet, there is 'piazza', which is a very great forum, for this kind of situation. Another example of that kind of external tool is 'slack', which is used for very specific communication context.

In the monolithic system, there may have some problems with the integration with the external tool. For example, in LMS, a teacher can structure an automatically graded exercise, and the student gets automatically graded result back when they put the answer. The teacher might use an external tool for doing that, but, as long as, the LMS do not have that privileges to connect the external tool with the LMS, the teacher has to put the result manually in the LMS, which is really a mess. Moreover, there is a chance to have human errors while putting the grade manually in the LMS.

The teachers do not want to explore to the net for different tools, rather using the tools of LMS provided by the university. Which is ended up instead of providing the best teacher providing the best tool, it provides the best teacher with the average tool and forces the teacher to use average quality resources. That is a problem because it reduces the motivation of excellent teaching.

Advantage of Monolithic System

Each university provides an LMS and they want the user to use it because it simplifies a lot of process in administrative level. For instance, the collection of grading, the definition of who are the student within a course, those thinks works well in the monolithic system. If a student takes a course in Blackboard, the moment he registered the course, his user account will show the course. This is great when teachers do not search for external tools. Teachers do not feel the extra responsibility to find out a greater tool as they have some defined tool in the LMS.

4.5.5 Security Benefits by this Shifting

The informants do not think this shifting increases any security benefits. Moreover, there may involve new challenges in the shared database.

Table 4.12: Quotation from the interview regarding the increased security benefits lead by the shifting

Theme	Participants Quotations
Security benefits of this shifting	"I do not think this shifting increases any security benefits, it just focuses on the probability of the system rather than the security." – Informant X "Using more resources in few place is beneficial for security" – Informant Y

Using more resources in few place is beneficial for security. For example, a software which has 10000 customers and they all are customizing their own security, which is cheaper. If one pull his own resources and can do more managing, more log analysis, make sure all the infrastructure is safe. Since pulling many resources, do not have to spend much, making the software service secure, if the software is everywhere. Pulling all the resource in one place and trying to make that place more secure is probably cheaper and trying to locally secure everything. Risk assessment is also necessary to prevent any risk.

A big provider could attract more expertise. However, the informant does not think anyone would have enough money to employ a security expert. To get a bigger efficiency one could have one more security experts.

4.5.6 Increased Security Risk of this Shifting

Though the informants do not see any security benefits of this shifting, this shifting might be a reason for a greater risk. Because in monolithic system everyone is using the same software. If anyone finds a security hole and would be able to use it all through the studies, and would be able to expand by telling somebody else about how he did and then it would just explode in usage. In some way, the security problem in the monolithic LMS would escalate much more quickly than a system putting together with different tools. The user can reuse their experience and the learning of the tools, despite this, they can also reuse the security problem, they might discover.

In e-learning ecosystem or cloud-based system, there is limited control over the infrastructure, the configuration. To have good configuration and good change management they have to rely on third parties.

Since this kind of system have everything is in one place there is potential for the leak between different customers or between different domains. Thus the system is more exposed for attacks. It could be difficult to do changes to prevent, or to close security holes, because the customer cannot take down the service, as often or as fastest. Moreover, attacks on someone else could influence all because all have almost the same infrastructure. The technical solution is making certificates configure controls.

Table 4.13: Quotation from interview regarding increased security issues lead by the shifting

Theme	Participants Quotations
Increased security risks leads by this shifting	“This shifting will increase security threats and will be difficult to find out and solve. Moreover, it will be an extra responsibility for the teacher to find out some good tool over the net, which may discourage them” - Informant X “Since the system has everything in one place there is potential for the leak between different customers or between different domains. The system is more exposed for attacks. It could be difficult to do changes to prevent, or to close security holes, because the customer can’t take down the service, as often or as fastest.” - Informant Y “This shifting will increase access and verification problem.” - Informant Z

To prevent security risks the security expert need to do a good job. Right people, right mindset, right expertise, and a good framework is needed for doing continues risk assessment and improve every day. One simple solution is, having good mindset helps to deal with technical issues and able to identify them and able to correct them.

4.6 Limitation

This section describes the limitation of this study. Avoiding error is completely impossible though care has been taken to eliminate the source of errors. The application of the result of this study is limited by the number of participants and their selection described in Section 4.6.1.

4.6.1 Participant selection

The participants of the questionnaire were recruited through the network of the author and the participants of the interview is recruited primarily from the network of Guttorm Sindre.

The participants of the survey are mainly from four different countries and the average number of the participant of each country is about 20. Only 20 participants for each country is not enough to represent the total view on the security of their e-learning system of a country. This number greatly limits how general the results of the study can be seen as.

The participants of the interview are mainly security focused people, yet they are not representative of the average IT-operative in Norway. This is the reason of both advantages and disadvantages. The main problem is the lack of representative data on the actual state of security in the organizations involved in Norway. As the participants are expected to be security focused, their answer is also high security focused. Having 3 participants greatly limits the result of this study and it is not the goal of qualitative study as it prefers higher number of participants.

4.6.2 Missing comment box below some questions

In the *Encountered Security Risk* part of the questionnaire there is a question about experienced unpermitted sharing of copyright material and getting wrong or false information from the e-learning system showing in Figure 3.18. The result shows that 16 participants faced more than once, and 9 participants faced the unpermitted sharing once in the e-learning system. This study needs to know more details about it from the participants, who faced the problem once or more than once. Same goes for the question 17 of the same Figure 3.18, which wants to know whether the students get any wrong or false information from the system. The result shows that 27 participants answered *rarely* and 9 participants answered *sometimes* they got false information from the e-learning system. This kind of question requires more comments depending on the respondents answer, to understand the security problem. While making the questionnaire if there would any option to write a paragraph under the two questions, then this two question might help more in this research to find out the security problem related to this, or to understand the problem. Only knowing how often they face this kind of problem could not help that much to know the problem.

4.7 Conclusion

Though this study has some limitation, it has focused on the security issues of e-learning system. The participants believe security could be violated most, in the asset - assignment; although it is not that much harmful to the system. While violation of security in admin account and the user account is more dangerous for the system. This research also shows that perceived security has a direct influence on perceived trust, which increases the acceptance of this kind of system to the customer. Moreover, experienced security problems and current security threats on the mentioned key assets are discussed here. This study shows that shifting from monolithic local system to e-learning ecosystem or cloud-based architecture does not provide any security benefits rather it solves scalability, integrity problem and ease some administrative process. On the other hand, this shifting increases the chance of security attacks and it becomes more difficult to prevent security holes.

Chapter 5

Conclusion and Future work

This chapter presents the concluding remarks of this thesis and discuss some recommendations for the future investigations.

5.1 Conclusion

This thesis has presented a case study on the security of the e-learning system. The Canadian students are mostly happy with the security of their e-learning system. 'Desire to Learn' is more secured e-learning system to it's user, comparing to the other e-learning system. This study also shows that security is a key determinant of user's trust. Secured e-learning system increases the usability of this kind of system. However it also shows that if the system do not maintain privacy then it will lose user's trust. User of the system thinks assignment is the asset which has more chance to violate confidentiality, integrity, and availability. This kind of violation is more harmful in admin account and user account. The user of the LMS mostly faced denial of service while accessing the assessment question in the e-exam. The key assets of the system is student's record, student's works, and personal information. Several mechanism is used to maintain and protect the assets, still there might have some minor risks. Shifting from traditional monolithic system to e-learning ecosystem or cloud-based architecture increases a lot of security threats. The possible threats are discussed in the study. New techniques are needed to mitigate the new threats in cost efficient way. Moreover, this research could be helpful for the people who want to work on the gathered security threats leads by this shifting.

5.1.1 Stakeholder's View on Security Challenges

Being the main user of e-learning system, student's feedback on security is important to ensure that the system is successfully implemented in the institution. The user of the system will feel more confident to use the system when the system developer and administrator will ensure that the system is error-free and secured. More attention should be given to the service and components which are exposed to security threats.

The participants' report has great variation in the security challenges. The conclusion based on the respondents' feedback are presented in this section.

Perceived Trust

Perceived security and perceived privacy are related to the perceived trust. When the perception of security is high, trust is a key determinant to behavioral intention. That means the user of the system will provide more personal and sensitive information to the system with less concern. User's trust can lead the e-learning system to a new direction as well as help to become the system more efficient. Thus, security features should be considered as an important issue, so that the e-learner use the e-learning system more willingly, when they perceive that the information provided during the securities transactions is secured and third parties will not have access to it.

Basic Security Properties and STRIDE Threat Model

The basic security properties are confidentiality, integrity, and availability. There is a link between this CIA triad and STRIDE threat model showed in Table 4.7. The relation is that violation of confidentiality is information disclosure, violation of integrity is tampering, and violation of availability is denial of service.

Confidentiality and Information Disclosure The result shows that the violation of confidentiality of *assignment* is in more critical position. The respondents believe that there is more chance of information disclosure in the asset assignment. The e-learning system has to be more secure and should have enough measure to keep the assignment confidential. The total result of the possibility of information disclosure shows that most of the respondent do not think it is possible to violate confidentiality or to disclose information of other asset.

The result also shows that the violation of confidentiality of admin account is more harmful. This violation has potential to violate the confidentiality of the whole e-learning process. All kind of security protection should be taken to prevent this kind of attack in admin account. Update the version of the system, security checking, and testing is required time to time to prevent information disclosure of admin account. The overall result of measuring harmfulness of violation of confidentiality shows that the participant believes violation of confidentiality in all of the assets is harmful. Thus the security measures is needed to protect all the assets from this kind of threat.

Integrity and Tampering The participants believe that tampering of assignment by the unauthorized user is easier in e-learning system, than other assets. The overall result shows that, the respondent answered neutral or unlikely in the possibility of tampering on all the mentioned assets. This result shows, there is less chance of tampering on all the other assets.

In the result of harmfulness scale, the user account is in the most critical position. That means the participants believe the violation of integrity in the user account is more harmful. Though the user account of e-learning system is still secure, one participant commented, it is possible to log in another user account in their e-learning system. If the system has some loophole, the provider need to solve it, otherwise, it will be a reason for a greater risk.

Availability and Denial of Service The result of the report shows that the respondent face availability problem mostly in the assignment (i.e. when they try to submit or download the assignment). This might happened for some other reason for instance, when the file extension does not match etc. If there is some problem with the server or the network then also the student failed to submit the assignment. The reason of the availability problem in the case of assignment should be investigated and solve, to make the e-learning system more efficient. The overall result of availability shows that the participant rarely faces availability problem or denial of service in the e-learning system. This is expected, as no system can not perform as it is expected because there may raise a lot of issues, like the network problem, server problem, sometimes different attacks can cause damage to the system. Student faces denial of service mostly in e-exam when they want to open the assessment question. It might take some time to open the question or some students might have some other problem when they want to open it.

The violation of confidentiality, integrity, and availability are mostly possible on the assets assignment, according to the answer of participants. That indicates student are facing problem while they are dealing with the assignments in this system. The result also shows that the respondents believe violating the confidentiality of admin account more harmful on the other hand violation of the integrity of user account is more harmful. This result is surprising because comparing to user account violating of integrity in admin account is more harmful. The reason behind this might be the focused stakeholder is the student, and they are sharing their views from their perspective.

5.1.2 Security Threats and Challenges

From the result of the interview, it is found that the participants of the system have experienced some threats like phishing attacks, identity theft by third parties, able to fool ‘the browser locking software’, able to get access to the system as a teacher. All of these previous security problems has been mitigated. Still, there might have possible threats. None of these threats is so much harmful to the total system and it could be solved other way around. Normally this kind of system does not provide a lot of money for security experts to check the security time to time. Still, it would be better for the system to do penetration testing after some fixed time to maintain good security.

Currently Blackboard are using as the e-learning system in NTNU. The challenges here is that Blackboard is a patch of a lot of software and if any security hole is found then it will not be possible for the system to fix up from bottom-up. Another problem of Blackboard is more related to the trade-off between functionality and security (i.e. the more tighten up the security, the less functionality the system has). This is the challenges reported from the interview.

Another interesting thing came out from the interview is that technical solution is not the only side for security measure. Because one can easily fool the system, which has a very good technical solution yet do not have the non-technical solution. Thus both technical and non-technical solution together can provide a better security solution. For example, in the e-exam, if the system has a good technical solution but, the student are talking with each other, or swapping their sits then the only good technical solution will not work. With the technical solution there should be some other non-technical solution like monitoring the examiners activity etc.

The result shows that e-learning system already experienced some minor security problems and the system might have some existing security threats. This kind of minor security threats should not be overlooked as they might have the potential to create a huge loss to the system. If any security holes are found in the system it should be immediately notified to the system developer so that it can be solved.

5.1.3 Shifting from Monolithic System to Cloud-based e-Learning Ecosystem

Though this shifting has solved the stability and integrity problem of the monolithic system, the informants do not find any security benefits from this shifting. Moreover, this shifting increases security threats in many ways. The findings of security threats of this shifting are - the limited control over the infrastructure and the configuration. As the system has to rely more on third parties, the system is more exposed for attacks. It could be difficult to do changes to prevent the security holes, because the customer cannot take down the service, as often or as fastest. Everyone is sharing same infrastructure in this kind of could-based system, thus attack on one system can affect all.

5.2 Future Work

The thesis has presented current security issues and challenges of the e-learning system. This study pointed out the security challenges and issues involve in the system. This would help the developer to develop the e-learning system more securely, even when the developer wants to shift the e-learning system to a new dimension. There is a need to see how the developer responds to the need. The further research will be on the subject of the developer's response to the security issues and challenges discussed in this research. The gathered security threats lead by the shifting from local monolithic system to e-learning ecosystem or cloud-based architecture, can be used to investigate more practically and theoretically. To make the modern e-learning ecosystem or cloud-based architecture more secure and efficient the security measure is a must. This study shows that the shifting is exposed for more attacks. New and economical technology is needed to make the security control easier, to make the e-learning system more advance as well as more secure further study should be done in this area. Analyzing the security issues and security challenges involve in e-learning system using questionnaire and interview among some participants are easy. However, a set of case studies on how the security challenges and issues are solved or could be solved, potentially increase the understanding of the security work in the public procurement. b

Bibliography

[1] V. Bevanda, J. Azemovic, and D. Music, “Privacy preserving in elearning environment (case of modeling hippocratic database structure)”, in *Informatics, 2009. BCI’09. Fourth Balkan Conference in*, IEEE, 2009, pp. 47–52.

[2] Z. F. Zamzuri, M. Manaf, Y. Yunus, and A. Ahmad, “Student perception on security requirement of e-learning services”, *Procedia-Social and Behavioral Sciences*, vol. 90, pp. 923–930, 2013.

[3] M. M. Gåsland, “Game mechanic based e-learning: A case study”, Master’s thesis, Department of Computer and Information Science, 2011.

[4] L Osin, “Integrating courseware with lessonware (computers in education)”, in *Information Technology, 1990.’Next Decade in Information Technology’, Proceedings of the 5th Jerusalem Conference on (Cat. No. 90TH0326-9)*, IEEE, 1990, pp. 657–659.

[5] R. K. Ellis, “A field guide to learning management system”, *American Society for Training & Development (ASTD)*, 2009.

[6] N Cavus, “Education technologies of the information age: Course management systems”, *Extend*, vol. 28, no. 2, 2008.

[7] Z. Ben Ami, “Knowledge practices environment (kpe)”, 2009.

[8] L. Vavik, S. Andersland, T. E. Arnesen, T. Arnesen, M. Espeland, I. Flatøy, P. Grønsdal Ingrid; Fadnes, S. Kjetil, and G. A. Tuset, “Skolefagsundersøkelsen”, Stord, Norge, Tech. Rep., 2009.

[9] M. Flavin, “Technology-enhanced learning and higher education”, *Oxford Review of Economic Policy*, vol. 32, no. 4, pp. 632–645, 2016.

[10] A. Sharm, *Discovering learning management systems: Basic functions and benefits*, [Online; accessed 28-June-2017], 2015. [Online]. Available: `https://elearningindustry.com/discovering-learning-management-systems-basic-functions-benefits`.

[11] *Learning management system (lms): Characteristics, functions and benefits*, [Online; accessed 28-June-2017]. [Online]. Available: `https://www.commlabindia.com/resources/article/lms.php`.

[12] *Encyclopaedia britannica*, [Online; accessed 19-October-2016]. [Online]. Available: `https://global.britannica.com/science/ecosystem`.

[13] V. Chang and L. Uden, “Governance for e-learning ecosystem”, in *2008 2nd IEEE International Conference on Digital Ecosystems and Technologies*, IEEE, 2008, pp. 340–345.

[14] M. Nasr and S. Ouf, “An ecosystem in e-learning using cloud computing as platform and web2. 0”, *The Research Bulletin of Jordan ACM*, vol. 2, pp. 134–140, 2011.

[15] V. Chang and C. Guetl, “E-learning ecosystem (eles) - a holistic approach for the development of more effective learning environment for small-and-medium sized enterprises (smes)”, *Digital EcoSystems and Technologies Conference*, 2007.

[16] B. Dong, Q. Zheng, J. Yang, H. Li, and M. Qiao, “An e-learning ecosystem based on cloud computing infrastructure”, in *Advanced Learning Technologies, 2009. ICALT 2009. Ninth IEEE International Conference on*, IEEE, 2009, pp. 125–127.

[17] R. Buyya, C. S. Yeo, and S. Venugopal, “Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities”, in *High Performance Computing and Communications, 2008. HPCC’08. 10th IEEE International Conference on*, Ieee, 2008, pp. 5–13.

[18] N. Wagner, K. Hassanein, and M. Head, “E-learning in higher education: A stakeholders’ analysis”, in *Information Technology Interfaces, 2006. 28th International Conference on*, IEEE, 2006, pp. 307–312.

[19] T Klobucar, M Jenabi, A Kaibel, and A Karapidis, “Security and privacy issues in technology enhanced learning”, *Expanding the Knowledge Economy: Issues, Applications, Case Studies*, pp. 1233–1240, 2007.

[20] Z. F. Zamzuri, M. Manaf, A. Ahmad, and Y. Yunus, “Computer security threats towards the e-learning system assets”, J. M. Zain, W. M. b. Wan Mohd, and E. El-Qawasmeh, Eds., pp. 335–345, 2011. DOI: `10.1007/978-3-642-22191-0_30`. [Online]. Available: `http://dx.doi.org/10.1007/978-3-642-22191-0_30`.

[21] E. Aïmeur, H. Hage, and F. S. M. Onana, “A framework for privacy-preserving e-learning”, in *IFIP International Conference on Trust Management*, Springer, 2007, pp. 223–238.

[22] Wikipedia, *Security — wikipedia, the free encyclopedia*, [Online; accessed 22-June-2017], 2017. [Online]. Available: `https://en.wikipedia.org/wiki/Security#cite_note-4`.

[23] G. McGraw, “Software security”, *IEEE Security & Privacy*, vol. 2, no. 2, pp. 80–83, 2004.

[24] J. Chirillo and E. Danielyan, *Sun certified security administrator for solaris 9 & 10 study guide*. McGraw-Hill, Inc., 2005.

[25] R Benjamin, B Gladman, and B. Randell, “Protecting it systems from cyber crime”, *The Computer Journal*, vol. 41, no. 7, pp. 429–443, 1998.

[26] C. Robson and K. McCartan, *Real world research*. John Wiley & Sons, 2016.

[27] *Google form*, `https://www.google.com/forms/about/`, Accessed: 2017-02-03.

[28] M. Galesic and M. Bosnjak, “Effects of questionnaire length on participation and indicators of response quality in a web survey”, *Public opinion quarterly*, vol. 73, no. 2, pp. 349–360, 2009.

[29] M. D. Myers and M. Newman, “The qualitative interview in is research: Examining the craft”, *Information and organization*, vol. 17, no. 1, pp. 2–26, 2007.

[30] S. Hannabuss, “Research interviews”, *New library world*, vol. 97, no. 5, pp. 22–30, 1996.

[31] J. Ritchie, J. Lewis, C. M. Nicholls, R. Ormston, *et al.*, *Qualitative research practice: A guide for social science students and researchers*. Sage, 2013.

[32] O. Doody and M. Noonan, “Preparing and conducting interviews to collect data”, *Nurse researcher*, vol. 20, no. 5, pp. 28–32, 2013.

[33] K. Kelley, B. Clark, V. Brown, and J. Sitzia, “Good practice in the conduct and reporting of survey research”, *International Journal for Quality in Health Care*, vol. 15, no. 3, pp. 261–266, 2003.

[34] M. Coughlan, P. Cronin, and F. Ryan, “Survey research: Process and limitations.”, *International Journal of Therapy & Rehabilitation*, vol. 16, no. 1, 2009.

[35] H. J. Rubin and I. S. Rubin, *Qualitative interviewing: The art of hearing data*. Sage, 2011.

[36] K. L. Easton, J. F. McComish, and R. Greenberg, “Avoiding common pitfalls in qualitative data collection and transcription”, *Qualitative health research*, vol. 10, no. 5, pp. 703–707, 2000.

[37] R. K. Yin, *Case study research: Design and methods. beverley hills*, 1984.

[38] H. A. Linstone, M. Turoff, *et al.*, *The delphi method: Techniques and applications*. Addison-Wesley Reading, MA, 1975, vol. 29.

[39] G. Rowe and G. Wright, “The delphi technique as a forecasting tool: Issues and analysis”, *International journal of forecasting*, vol. 15, no. 4, pp. 353–375, 1999.

[40] S. W. Normannsen. (2015). E-læringsfadesen: Itslearning vil ikke godta avlysningen, [Online]. Available: `http://www.universitetsavisa.no/campus/article40403.ece` (visited on 05/17/2017).

[41] J. Carlos Roca, J. José García, and J. José de la Vega, “The importance of perceived trust, security and privacy in online trading systems”, *Information Management & Computer Security*, vol. 17, no. 2, pp. 96–113, 2009.

[42] S. L. Jarvenpaa and P. A. Todd, “Consumer reactions to electronic shopping on the world wide web”, *International journal of electronic commerce*, vol. 1, no. 2, pp. 59–88, 1996.

[43] R. K. Chellappa and P. A. Pavlou, “Perceived information security, financial liability and consumer trust in electronic commerce transactions”, *Logistics Information Management*, vol. 15, no. 5/6, pp. 358–368, 2002.

[44] R. Kalakota and A. B. Whinston, *Electronic commerce: A manager’s guide*. Addison-Wesley Professional, 1997.

[45] D. C. Arnott, D. Wilson, A. Mukherjee, and P. Nath, “Role of electronic trust in online retailing: A re-examination of the commitment-trust theory”, *European Journal of Marketing*, vol. 41, no. 9/10, pp. 1173–1202, 2007.

[46] E. G. Carmines and R. A. Zeller, *Reliability and validity assessment*. Sage publications, 1979, vol. 17.

[47] J. Nunnally and I. Bernstein, “Psychometric theory mcgraw-hill new york google scholar”, 1978.

[48] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error", *Journal of marketing research*, pp. 39–50, 1981.

[49] E. J. Pedhazur, "Multiple regression in behavioral research: Explanation and prediction", 1997.

[50] *Example of very simple path analysis via regression (with correlation matrix input)*, `http://psych.unl.edu/psycrs/statpage/pathex1.pdf`.

[51] S. S. Greene, *Security policies and procedures.* New Jersey: Pearson Education, 2006.

[52] Wikipedia, *Stride(security) — wikipedia, the free encyclopedia*, [Online; accessed 09-March-2017], 2016. [Online]. Available: `https://en.wikipedia.org/wiki/STRIDE_(security)`.

[53] OWASP, *Application threat modeling*, [Online; accessed 02-May-2017], 2015. [Online]. Available: `https://www.owasp.org/index.php/Application_Threat_Modeling`.

[54] Microsoft, *The stride threat model*, [Online; accessed 10-March-2017], 2016. [Online]. Available: `https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx`.

[55] *Repudiation attack*, [Online; accessed 08-December-2016], 2016. [Online]. Available: `https://www.owasp.org/index.php/Repudiation_Attack`.

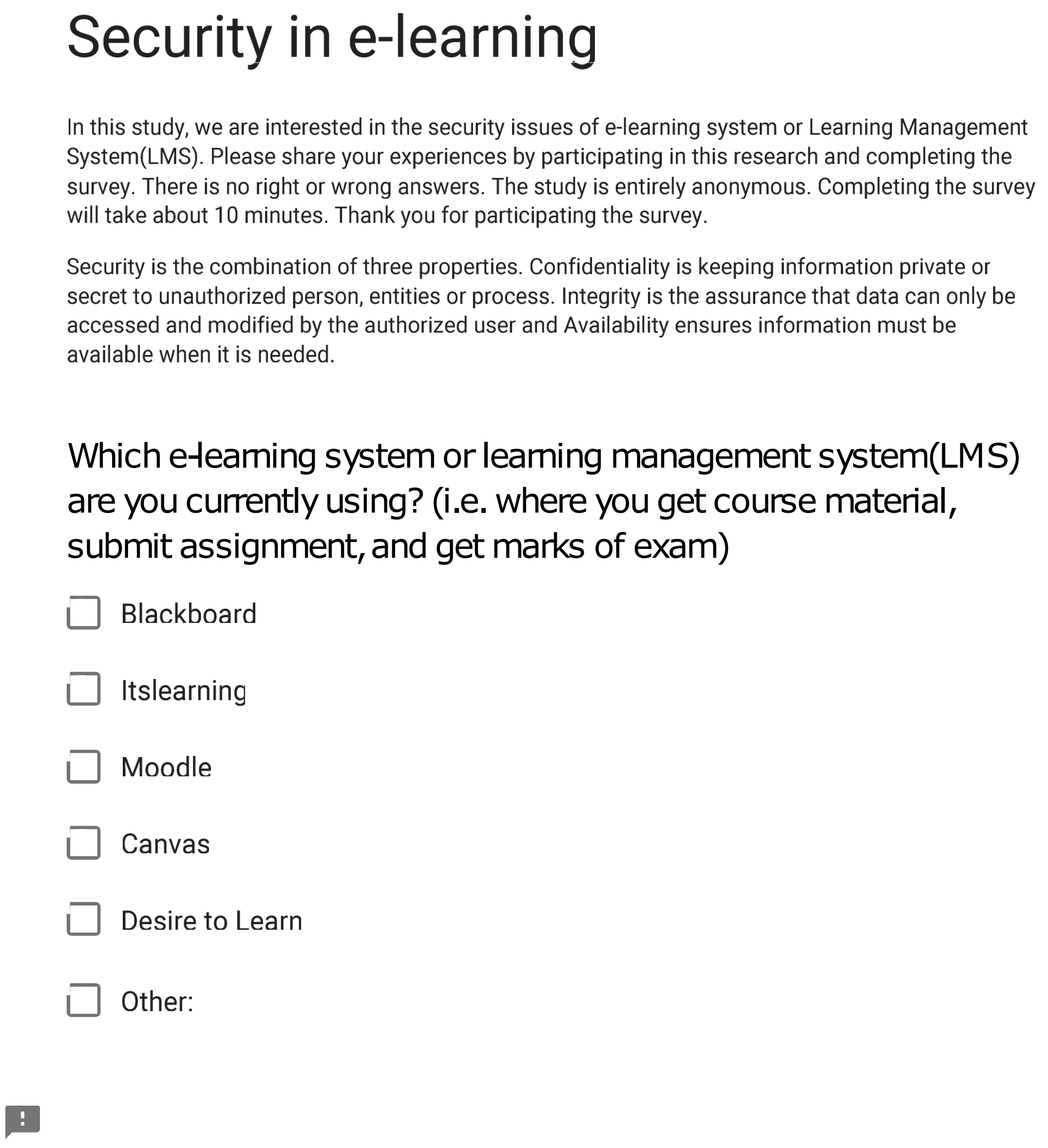
[56] Wikipedia, *Denial-of-service attack — wikipedia, the free encyclopedia*, [Online; accessed 08-December-2016], 2016. [Online]. Available: `https://en.wikipedia.org/wiki/Denial-of-service_attack`.

Appendices

Appendix A

Questionnaire

This appendix includes the questionnaire which is sent to the participants. It is presented here in the exact form the participants saw when answering it. The questionnaire has five parts, which are shown below.



Security in e-learning

In this study, we are interested in the security issues of e-learning system or Learning Management System(LMS). Please share your experiences by participating in this research and completing the survey. There is no right or wrong answers. The study is entirely anonymous. Completing the survey will take about 10 minutes. Thank you for participating the survey.

Security is the combination of three properties. Confidentiality is keeping information private or secret to unauthorized person, entities or process. Integrity is the assurance that data can only be accessed and modified by the authorized user and Availability ensures information must be available when it is needed.

Which e-learning system or learning management system(LMS) are you currently using? (i.e. where you get course material, submit assignment, and get marks of exam)

□ Blackboard

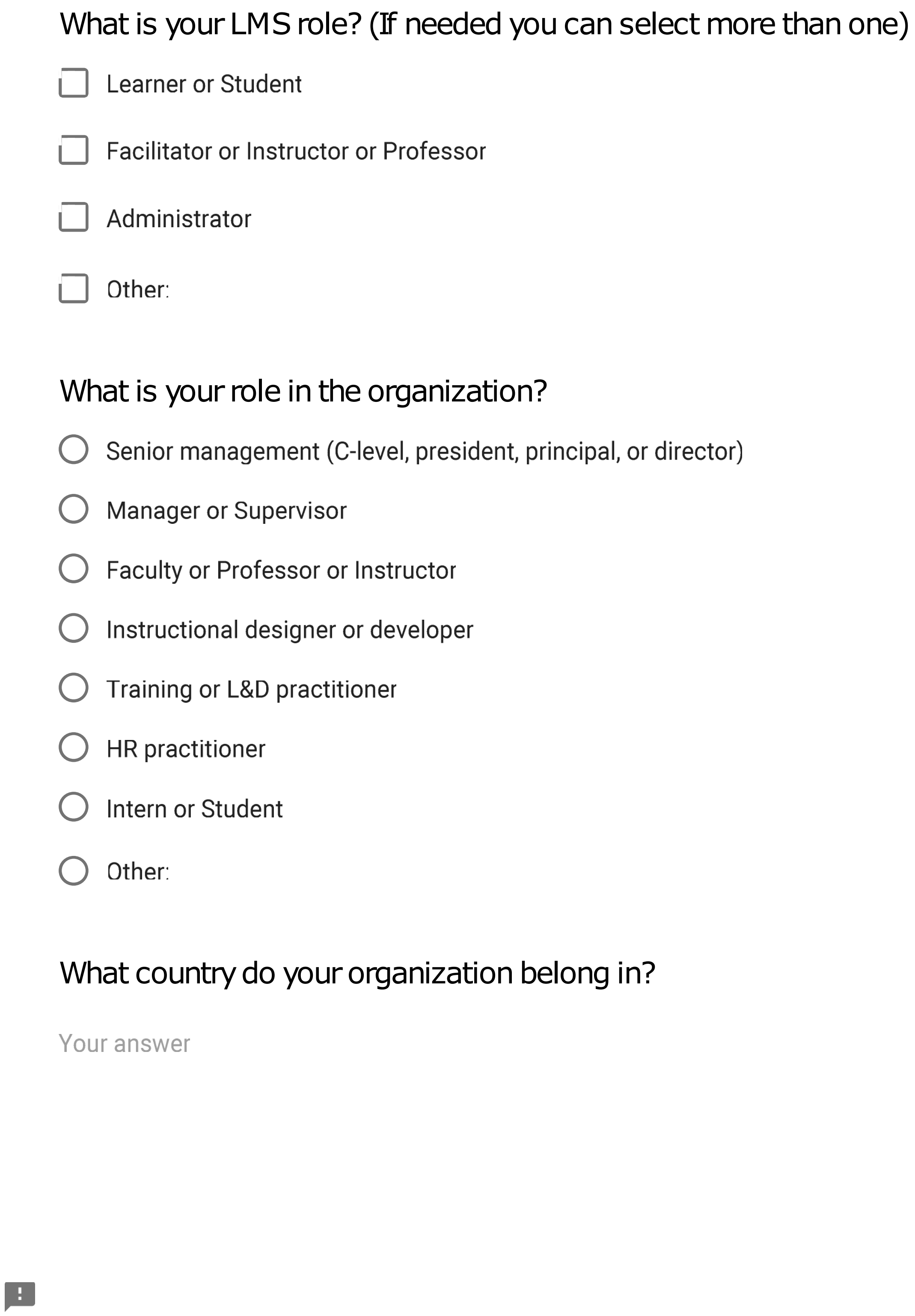
□ Itslearning

□ Moodle

□ Canvas

□ Desire to Learn

□ Other:



What is your LMS role? (If needed you can select more than one)

□ Learner or Student

□ Facilitator or Instructor or Professor

□ Administrator

□ Other:

What is your role in the organization?

○ Senior management (C-level, president, principal, or director)

○ Manager or Supervisor

○ Faculty or Professor or Instructor

○ Instructional designer or developer

○ Training or L&D practitioner

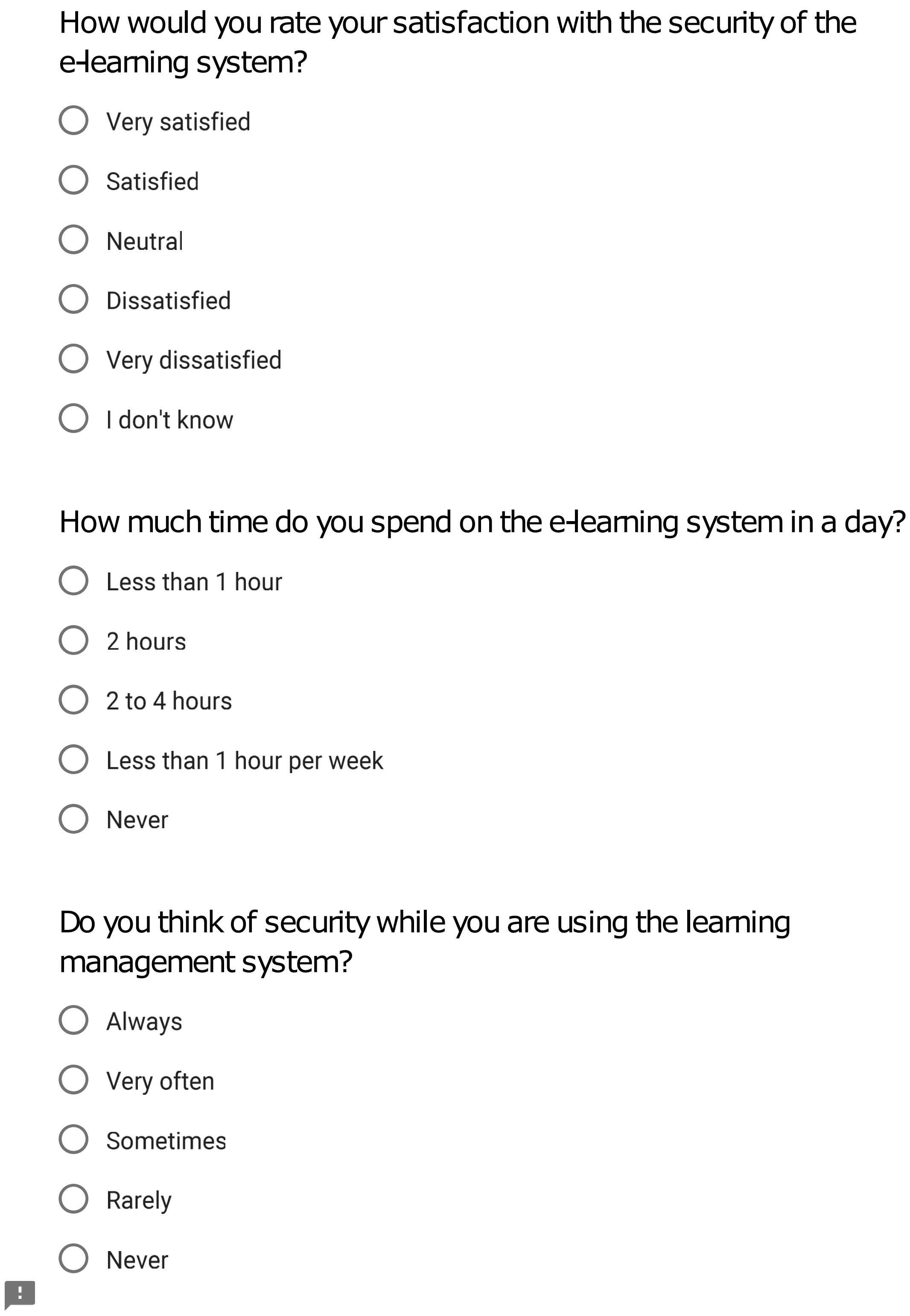
○ HR practitioner

○ Intern or Student

○ Other:

What country do your organization belong in?

Your answer



How would you rate your satisfaction with the security of the e-learning system?

○ Very satisfied

○ Satisfied

○ Neutral

○ Dissatisfied

○ Very dissatisfied

○ I don't know

How much time do you spend on the e-learning system in a day?

○ Less than 1 hour

○ 2 hours

○ 2 to 4 hours

○ Less than 1 hour per week

○ Never

Do you think of security while you are using the learning management system?

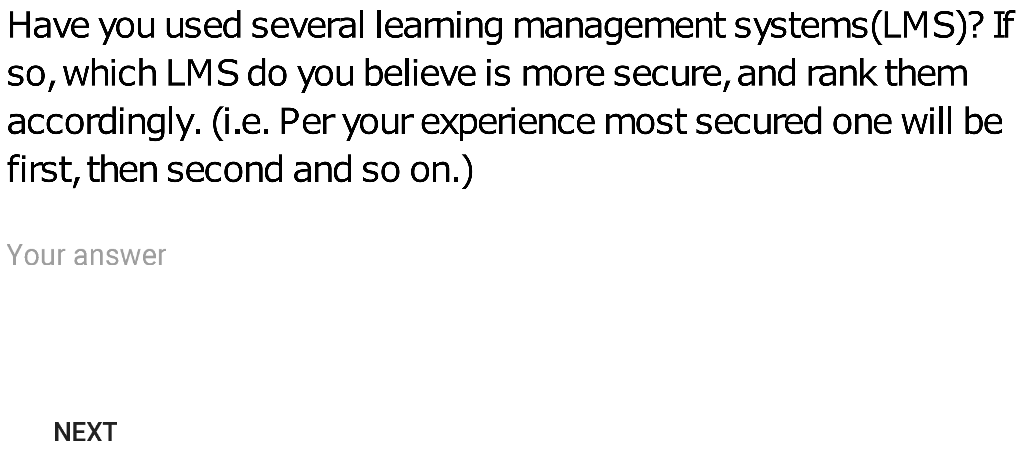
○ Always

○ Very often

○ Sometimes

○ Rarely

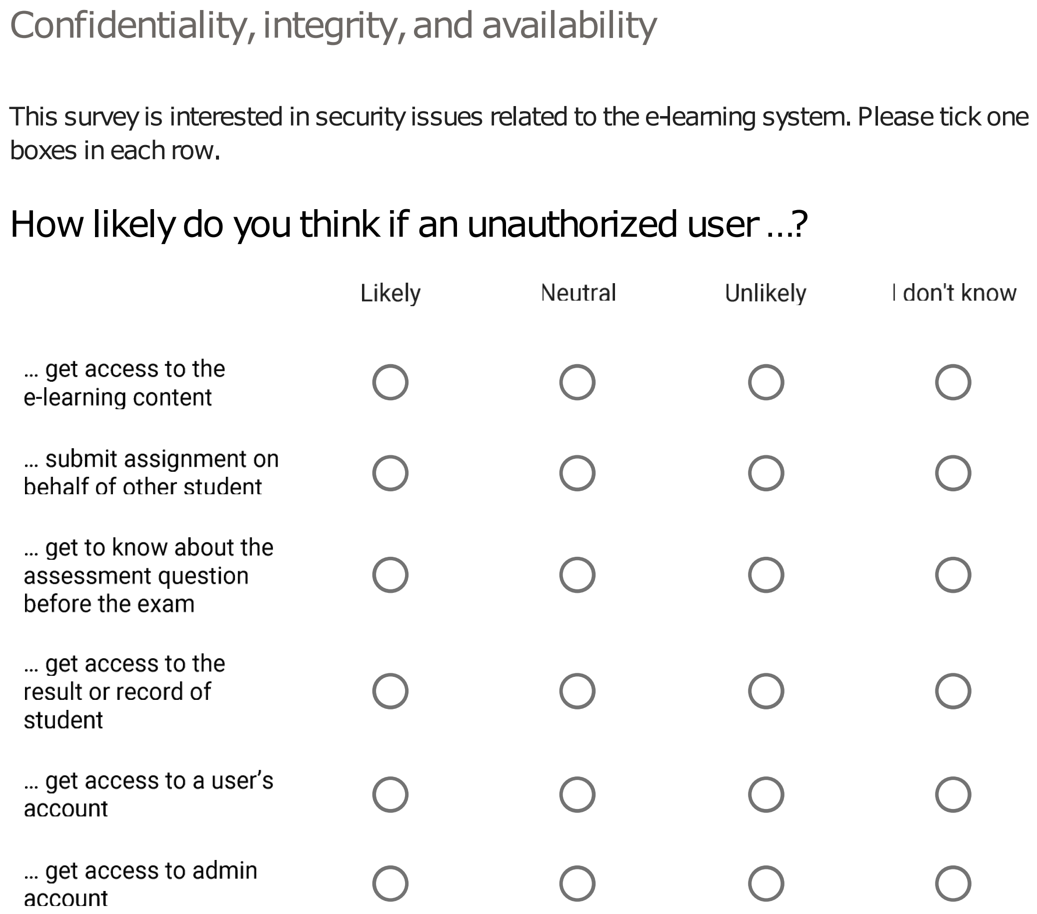
○ Never



Have you used several learning management systems(LMS)? If so, which LMS do you believe is more secure, and rank them accordingly. (i.e. Per your experience most secured one will be first, then second and so on.)

Your answer

Figure A.1: Introductory and basic part of the questionnaire

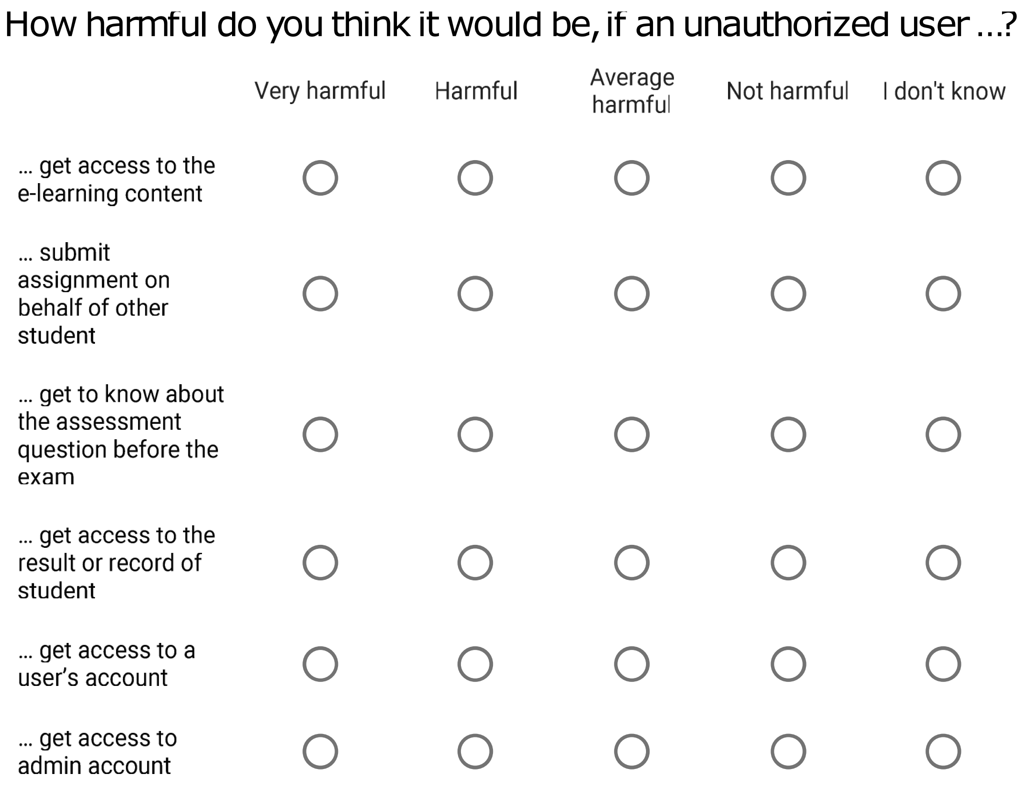


Confidentiality, integrity, and availability

This survey is interested in security issues related to the e-learning system. Please tick one boxes in each row.

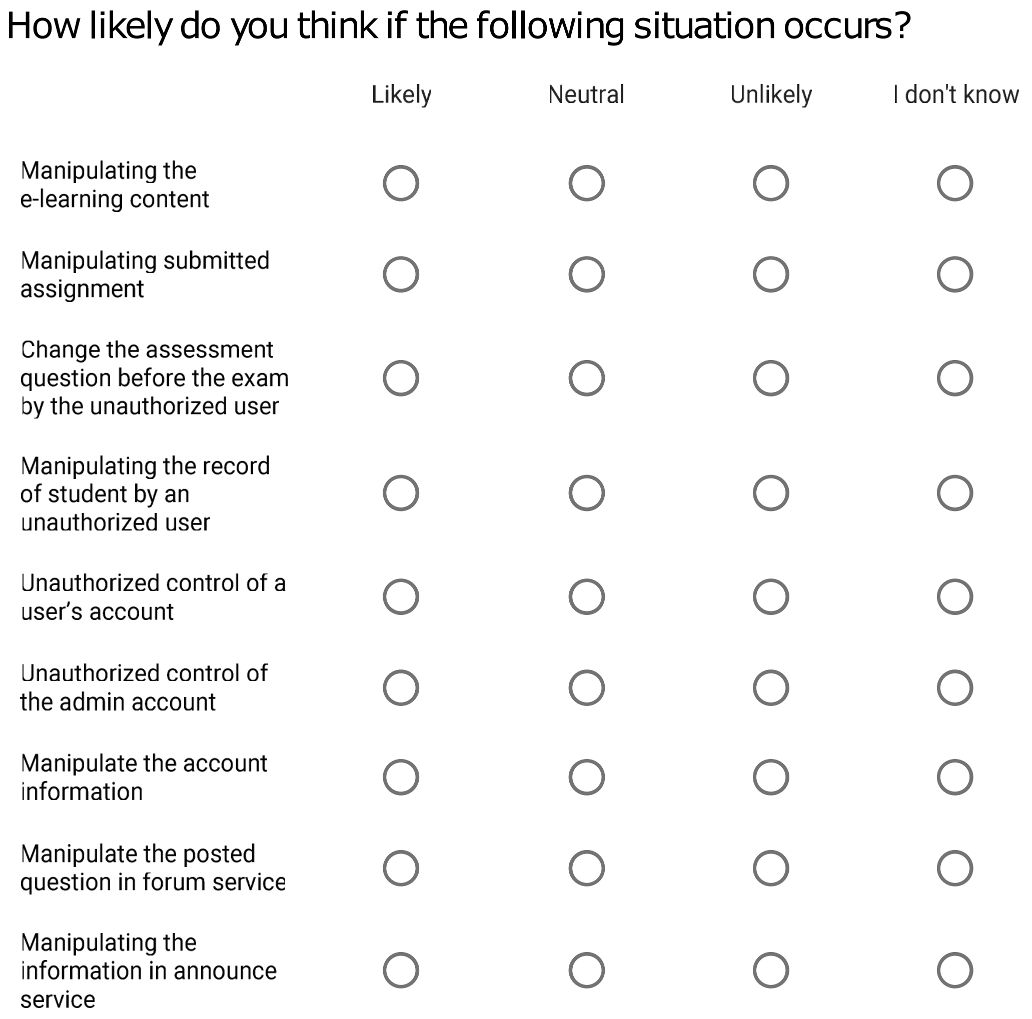
How likely do you think if an unauthorized user …?

	Likely	Neutral	Unlikely	I don't know
… get access to the e-learning content	○	○	○	○
… submit assignment on behalf of other student	○	○	○	○
… get to know about the assessment question before the exam	○	○	○	○
… get access to the result or record of student	○	○	○	○
… get access to a user’s account	○	○	○	○
… get access to admin account	○	○	○	○



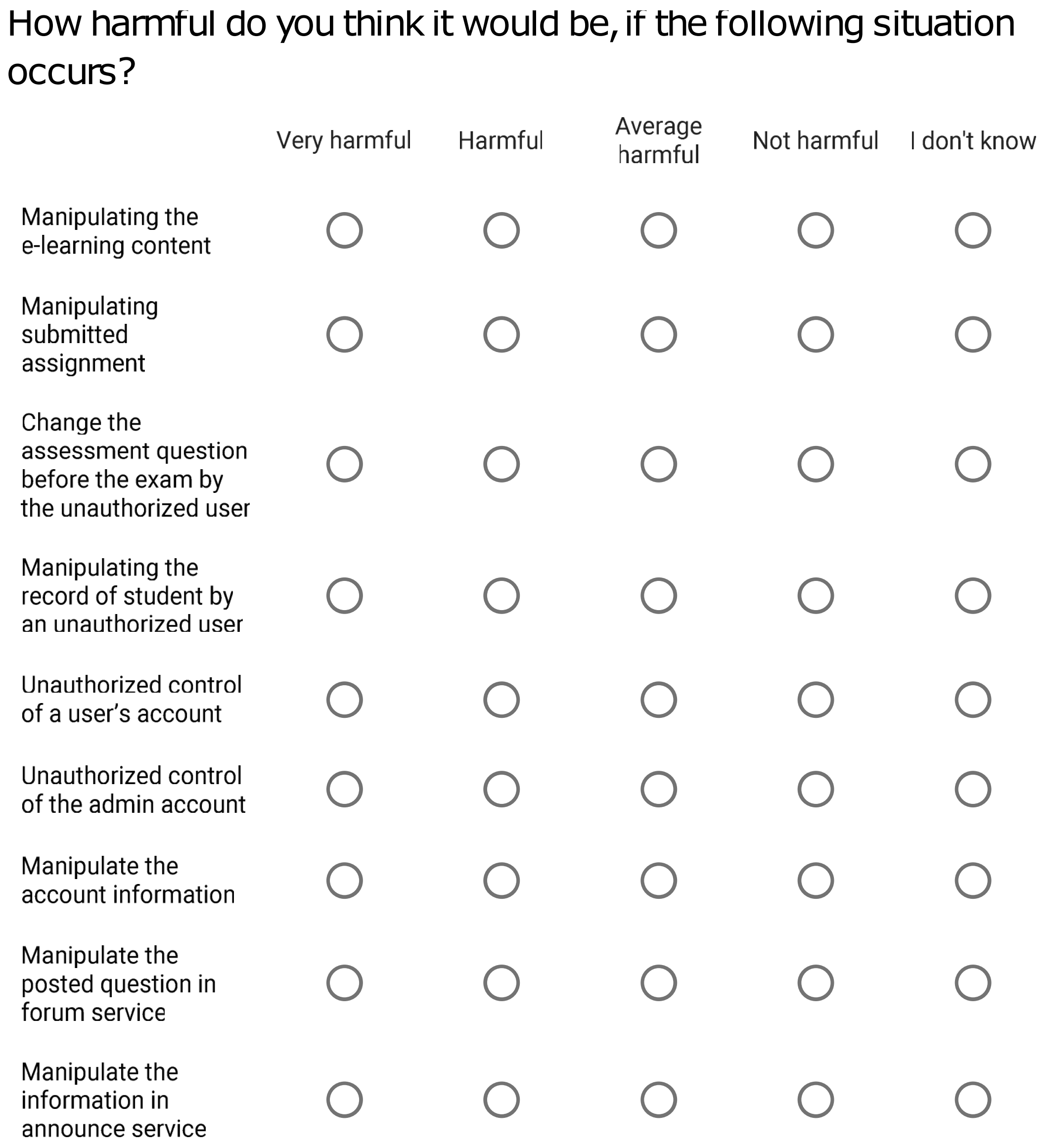
How harmful do you think it would be, if an unauthorized user …?

	Very harmful	Harmful	Average harmful	Not harmful	I don't know
… get access to the e-learning content	○	○	○	○	○
… submit assignment on behalf of other student	○	○	○	○	○
… get to know about the assessment question before the exam	○	○	○	○	○
… get access to the result or record of student	○	○	○	○	○
… get access to a user’s account	○	○	○	○	○
… get access to admin account	○	○	○	○	○



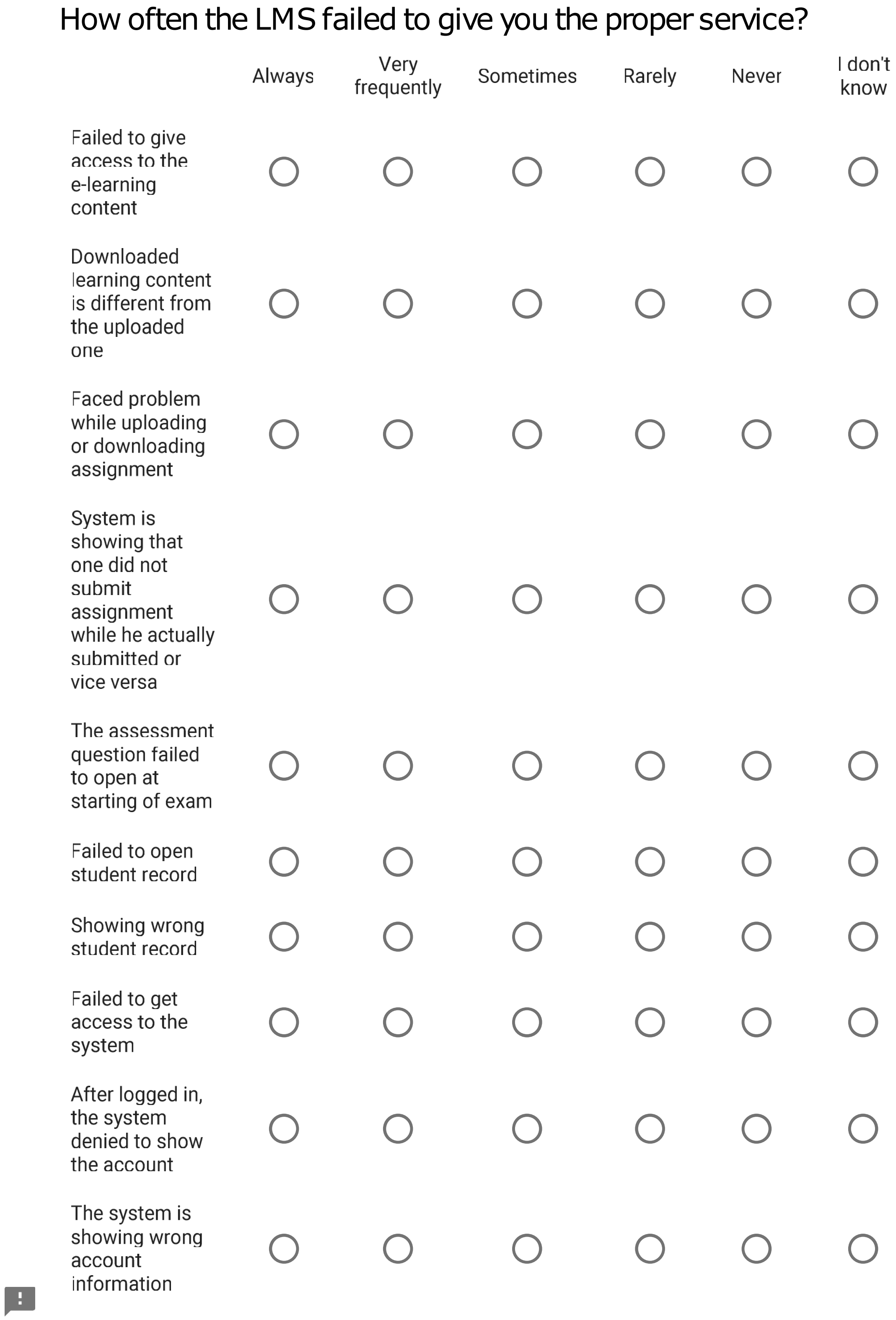
How likely do you think if the following situation occurs?

	Likely	Neutral	Unlikely	I don't know
Manipulating the e-learning content	○	○	○	○
Manipulating submitted assignment	○	○	○	○
Change the assessment question before the exam by the unauthorized user	○	○	○	○
Manipulating the record of student by an unauthorized user	○	○	○	○
Unauthorized control of a user’s account	○	○	○	○
Unauthorized control of the admin account	○	○	○	○
Manipulate the account information	○	○	○	○
Manipulate the posted question in forum service	○	○	○	○
Manipulating the information in announce service	○	○	○	○



How harmful do you think it would be, if the following situation occurs?

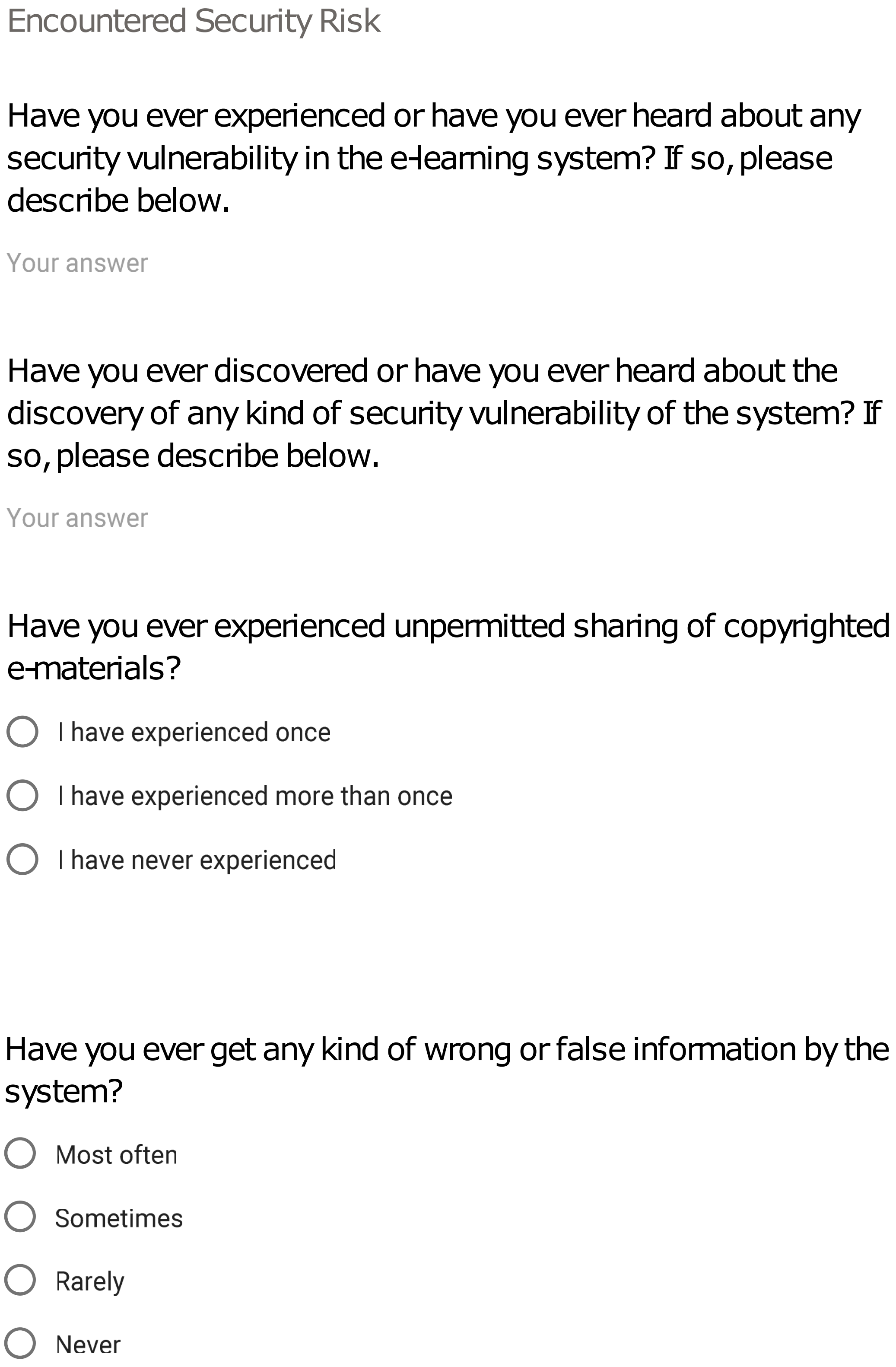
	Very harmful	Harmful	Average harmful	Not harmful	I don't know
Manipulating the e-learning content	○	○	○	○	○
Manipulating submitted assignment	○	○	○	○	○
Change the assessment question before the exam by the unauthorized user	○	○	○	○	○
Manipulating the record of student by an unauthorized user	○	○	○	○	○
Unauthorized control of a user’s account	○	○	○	○	○
Unauthorized control of the admin account	○	○	○	○	○
Manipulate the account information	○	○	○	○	○
Manipulate the posted question in forum service	○	○	○	○	○
Manipulate the information in announce service	○	○	○	○	○



How often the LMS failed to give you the proper service?

	Always	Very frequently	Sometimes	Rarely	Never	I don't know
Failed to give access to the e-learning content	○	○	○	○	○	○
Downloaded learning content is different from the uploaded one	○	○	○	○	○	○
Faced problem while uploading or downloading assignment	○	○	○	○	○	○
System is showing that one did not submit assignment while he actually submitted or vice versa	○	○	○	○	○	○
The assessment question failed to open at starting of exam	○	○	○	○	○	○
Failed to open student record	○	○	○	○	○	○
Showing wrong student record	○	○	○	○	○	○
Failed to get access to the system	○	○	○	○	○	○
After logged in, the system denied to show the account	○	○	○	○	○	○
The system is showing wrong account information	○	○	○	○	○	○

Figure A.2: Basic security risk



Encountered Security Risk

Have you ever experienced or have you ever heard about any security vulnerability in the e-learning system? If so, please describe below.

Your answer

Have you ever discovered or have you ever heard about the discovery of any kind of security vulnerability of the system? If so, please describe below.

Your answer

Have you ever experienced unpermitted sharing of copyrighted e-materials?

○ I have experienced once

○ I have experienced more than once

○ I have never experienced

Have you ever get any kind of wrong or false information by the system?

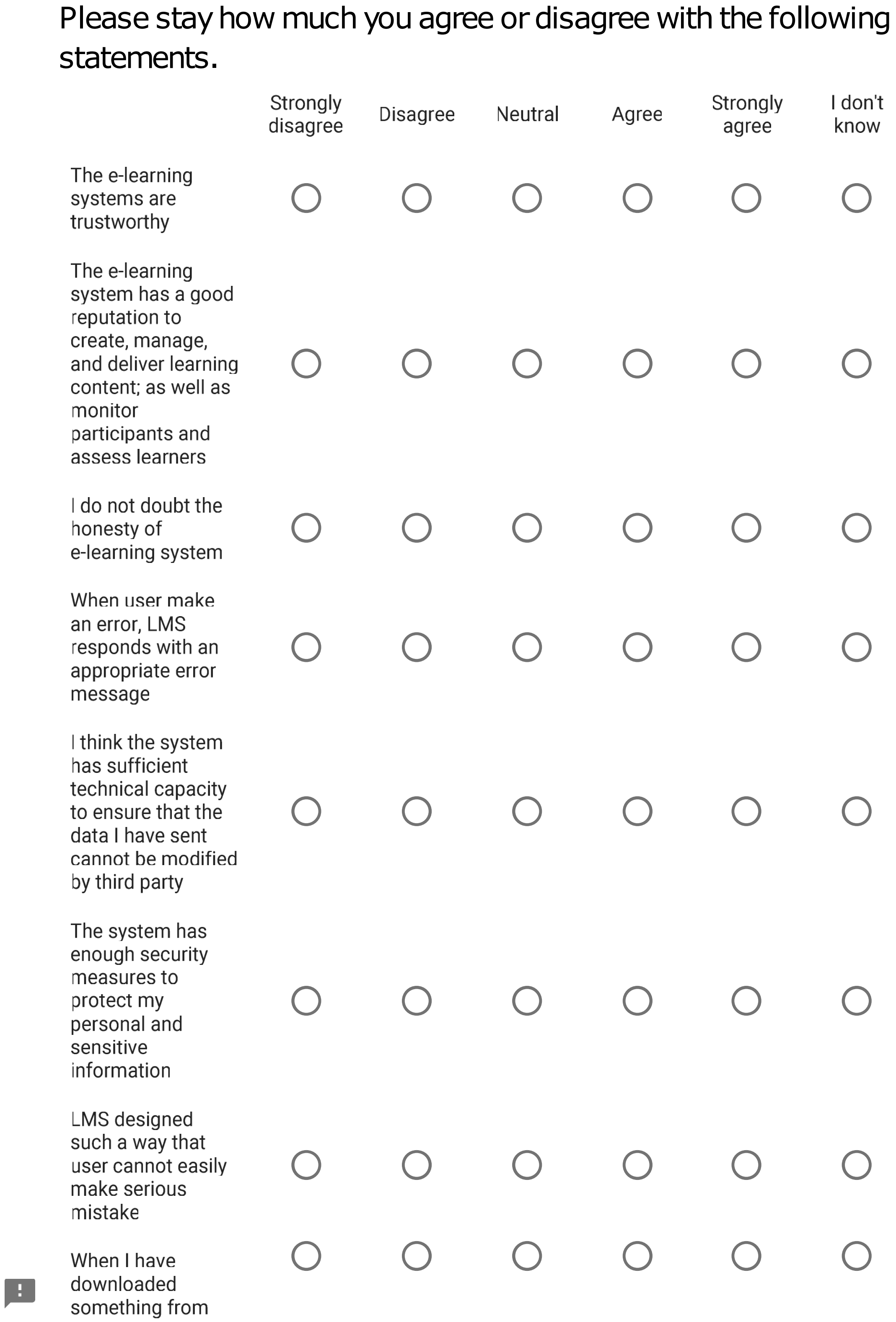
○ Most often

○ Sometimes

○ Rarely

○ Never

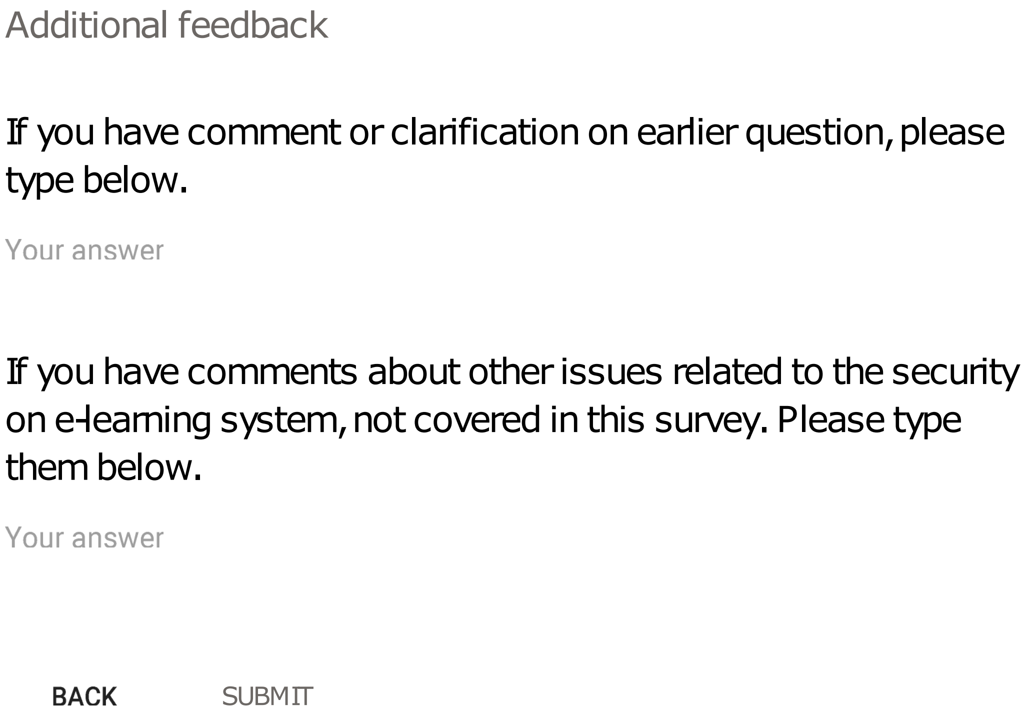
Figure A.3: Encountered security risk



Please stay how much you agree or disagree with the following statements.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	I don't know
The e-learning systems are trustworthy	○	○	○	○	○	○
The e-learning system has a good reputation to create, manage, and deliver learning content; as well as monitor participants and assess learners	○	○	○	○	○	○
I do not doubt the honesty of e-learning system	○	○	○	○	○	○
When user make an error, LMS responds with an appropriate error message	○	○	○	○	○	○
I think the system has sufficient technical capacity to ensure that the data I have sent cannot be modified by third party	○	○	○	○	○	○
The system has enough security measures to protect my personal and sensitive information	○	○	○	○	○	○
LMS designed such a way that user cannot easily make serious mistake	○	○	○	○	○	○
When I have downloaded something from	○	○	○	○	○	○

Figure A.4: Measuring perceived trust



Additional feedback

If you have comment or clarification on earlier question, please type below.

Your answer

If you have comments about other issues related to the security on e-learning system, not covered in this survey. Please type them below.

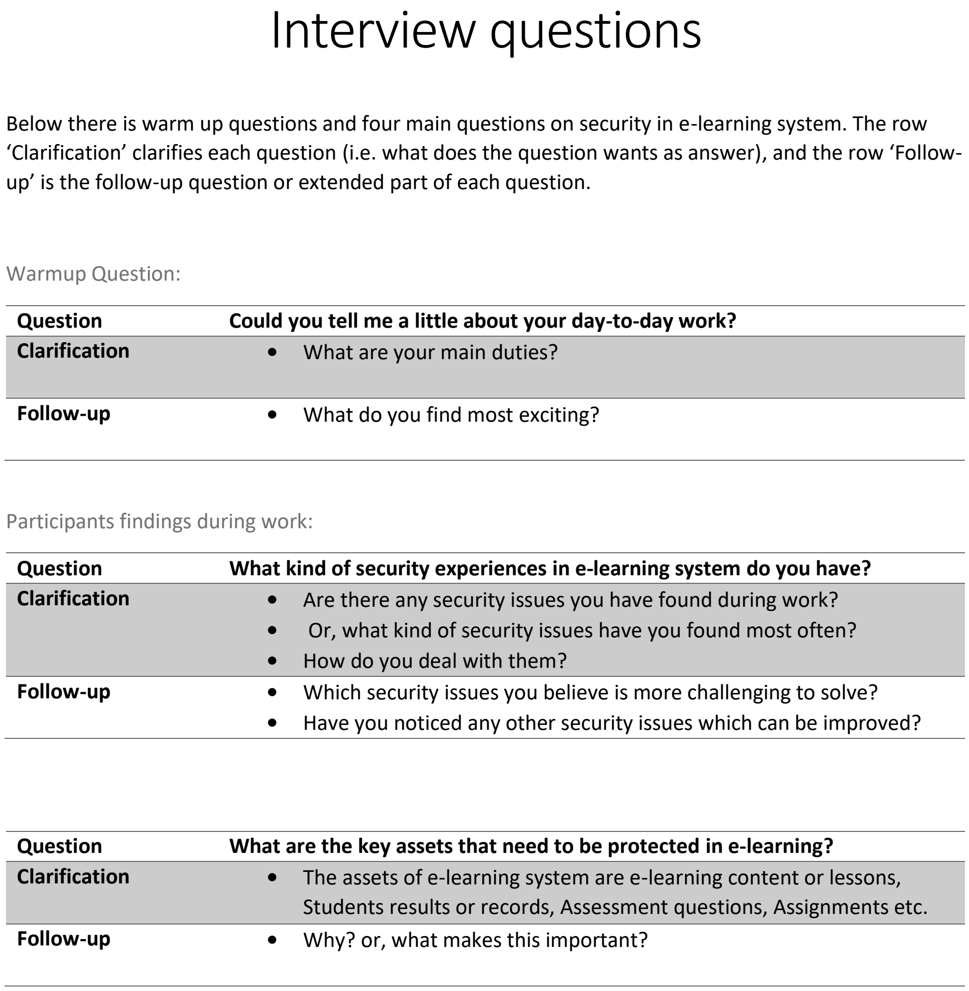
Your answer

Figure A.5: Additional feedback

Appendix B

Interview Questions

A interview guide are made before the interview. The questions which were asked during the interviews, are presented in this appendix. The guide has four parts, they are warm-up questions, participants finding during work, main body of the questionnaire, and closing questions. Each question has two rows one is clarification, another one is follow-up. The row *Clarification* clarifies each question (i.e. what does the question wants as answer), and the row *Follow-up* is the follow-up question or extended part of each question.



Interview questions

Below there is warm up questions and four main questions on security in e-learning system. The row 'Clarification' clarifies each question (i.e. what does the question wants as answer), and the row 'Follow-up' is the follow-up question or extended part of each question.

Warmup Question:

Question	**Could you tell me a little about your day-to-day work?**
Clarification	• What are your main duties?
Follow-up	• What do you find most exciting?

Participants findings during work:

Question	**What kind of security experiences in e-learning system do you have?**
Clarification	• Are there any security issues you have found during work? • Or, what kind of security issues have you found most often? • How do you deal with them?
Follow-up	• Which security issues you believe is more challenging to solve? • Have you noticed any other security issues which can be improved?

Question	**What are the key assets that need to be protected in e-learning?**
Clarification	• The assets of e-learning system are e-learning content or lessons, Students results or records, Assessment questions, Assignments etc.
Follow-up	• Why? or, what makes this important?

Main Question:

Question	What are the security threats to the e-learning system?
Clarification	• Security threats are the possible danger which can harm the e-learning system. • How are they harmful to the e-learning system?
Follow-up	• What is the best way to solve them?

Question	What do you think about shifting this learning system from traditional monolithic system to modern e-learning ecosystem or cloud based system?
Clarification	• What is the big differences between these two systems? • Which one is more efficient for the educational institution? Why?
Follow-up	• What are the advantages of these two systems? • What are the disadvantages of these systems?

Question	How do you describe this shifting from traditional system to modern learning system as an opportunity to improve security?
Clarification	• Is this shifting increased the security benefits? • Or, is this shifting reduces any security risk? • What are the security benefits we can get from this shifting?

Question	What are the increased security threats you believe leads by this shifting?
Clarification	• Is this shifting leads to any security risks?
Follow-up	• How to solve the problems? • Some student tried to cheat before, and so now. Maybe the process of cheating has changed but still, people are finding out new ways to cheat the system. In that case is this shifting has some advantage to protect from cheating?

Closing Question:

Question	Do you have anything else you would like to talk about, that you don’t feel you have had the opportunity to talk about so far?