Digital Learning Security Issues in Cloud Based E-Learning for Higher Education Institutions: An Overview

Azliza Yacob[1*], Noraida Hj Ali[2*], Noor Suhana Sulaiman[3], Nur Sukinah Aziz[4]

[1, 3, 4] *University College TATI, Kemaman, Terengganu, Malaysia*

[2] *University Malaysia Terengganu, Kuala Terengganu, Terengganu, Malaysia*

Abstract:- Digital learning has become an integral part of education, and cloud-based e-learning platforms have gained popularity due to their flexibility, scalability, and cost-effectiveness. During pandemic COVID-19, an online learning initiative was recommended; thus, the role of the internet became important without realizing the online risks and how people should respond properly to the mentioned risks. Thus, the purpose of this paper is to provide an overview of the security issues in cloud-based e-learning for Higher Education Institutions. There are many potential risks and threats posed by internet harassment and inappropriate usage of personal information, which may lead to network security issues. Lecturers, instructors, and students download and upload many things for the purpose of education without being aware of the security level. It shows the lack of user awareness of the fundamentals of internet knowledge, which may lead to network security issues. This study also conducted a preliminary study to get an overview of the use of cloud-based e-learning in higher education in Malaysia, which was the main factor motivating for the future study. Cloud-based e-learning platforms offer numerous benefits to higher education institutions, but they also present security challenges that must be addressed. Institutions must implement appropriate security measures to protect their students, faculty, and intellectual property from security threats. This initial research will help us design a Digital Learning Security Model for Enhancing e-Learning Privacy and Data Protection based on UTAUT in Higher Education institutions.

Keywords: *digital learning, cloud computing, cloud-based e-learning, security issue.*

1. Introduction

In comparison to traditional classroom-based learning, e-learning has grown in popularity recently, particularly in higher education institutions. The ability to access educational material from any location at any time gives learners greater flexibility and convenience. Online education research is focusing a lot of attention on how common online learning is and how to create a productive online learning environment. By using cloud computing to distribute educational content, cloud-based e-learning advances e-learning. Institutions can more easily manage instructional resources and give students access from anywhere as a result. Scalability, affordability, and accessibility are other advantages of cloud-based e-learning platforms. When necessary, institutions can quickly increase or decrease their resource allocation, and students can access educational resources from anywhere.

E-learning solutions that are cloud-based also provide advantages, including scalability, affordability, and accessibility. Students can access educational information on any device with an internet connection, and institutions can quickly scale up or down their resources as necessary. There are numerous advantages to e-learning that make education more convenient, effective, and accessible. Adaptive technologies provide personalised e-learning, which customises content to meet the needs of each learner and improves overall learning outcomes. Institutions may reach a wide audience thanks to e-learning's scalability, and the integration of various multimedia resources and real-time updates guarantees the delivery of engaging and up-to-date content.

But, as was already indicated, there are security issues with cloud-based e-learning that must be resolved. In order to assess the security concerns related to cloud-based e-learning for higher education institutions, this study was done. Five sections make up the debate in this paper. The introduction is in Section 1, the research background is in Section 2, the research methodologies are discussed in Section 3, the privacy and data protection in cloud-based e-learning is discussed in Section 4, the result of a preliminary study is discussed in Section 5, and the conclusion is discussed in Section 6.

2. Research Background

The rapid changes in the world today have brought improvements in today's educational environment. By giving students access to material quickly and with high accuracy, digital learning seeks to open up new avenues for academic endeavours. It can help students perform better and get more knowledge, experience, and motivation. Additionally, there's a good chance it will improve communication between teachers and pupils[1]. According to [2] e-learning encourages diversity by enabling people to access educational materials from almost anywhere, regardless of their physical location. Because of its flexibility, students can move at their own speed, fitting a variety of schedules and learning preferences. One important benefit is cost-effectiveness, which lowers the costs related to conventional classroom arrangements. As a result of technical improvements and the widespread usage of cloud computing, digital learning has significantly gained traction in recent years, notably in higher education institutions. The widespread of internet brought countless benefits to the world with powerful tool for communication [3] without realizing the risks and actions that should be taken while online [4][5]. Higher education institutions are rapidly utilizing cloud-based e-learning platforms because of their adaptability, scalability, and affordability. To maintain the security of student data and intellectual property, these platforms also create security issues that must be resolved.

The security problems posed by e-learning platforms that operate in the cloud have been the subject of several studies. For instance, data security and privacy were found to be the main issues with cloud-based e-learning platforms in a study by [6]. To maintain data security and privacy, the report advised organizations to adopt encryption, access restriction, and other security measures. [7] used a list of cloud applications to analyze how security continues to be a possible issue for cloud users around the world. This study found that if risks are considered right away, the topic of solutions can be divided into four pillars: visibility, compute-based security, network protection, and finally identity security. This will help us build a more thorough knowledge base.

A study by [8] also looked at the security issues with cloud-based e-learning platforms from the viewpoint of professors. The study revealed a number of issues, including the need for training on how to use secure e-learning platforms and the establishment of institutional rules to safeguard student information and intellectual property. Other issues included a lack of knowledge about security concerns. The COVID-19 pandemic presented various security issues with cloud-based e-learning platforms, according to a study by [9]. The study emphasized the significance of putting in place suitable security precautions, like secure video conferencing systems and VPNs, to guarantee the security of student information and intellectual property. Cloud-based e-learning platforms offer various benefits, such as scalability, accessibility, and cost-effectiveness.

To protect the confidentiality, integrity, and accessibility of sensitive educational data and resources, they also carry with them a number of security concerns that need to be resolved. For higher education institutions, the following study background for some of the digital learning security issues in cloud-based e-learning and their elaboration:

- **Data breaches:** Cloud-based e-learning systems store a lot of sensitive data, such as student records, financial information, and intellectual property. This data is vulnerable to breaches if the cloud provider's security measures are not adequate [10].
    - This can happen due to a number of factors, such as:
        - **Weak passwords:** If users choose weak passwords or reuse passwords across multiple accounts, it can make it easier for hackers to gain access to their accounts.

- **Phishing attacks:** Phishing attacks are a common way for hackers to steal personal information. In a phishing attack, the hacker sends an email or text message that appears to be from a legitimate source, such as a bank or credit card company. The email or text message will often contain a link that, when clicked, will take the user to a fake website that looks like the real website. Once the user enters their personal information on the fake website, the hacker can steal it.
- **Software vulnerabilities:** Software vulnerabilities are flaws in software that can be exploited by hackers to gain access to a system. Cloud providers regularly update their software to fix vulnerabilities, but it is important for users to keep their software up-to-date as well.

- **Denial-of-service (DoS) attacks:** DoS attacks can overwhelm a cloud-based e-learning system with traffic, making it unavailable to users. This can disrupt classes and prevent students from accessing their coursework [11].
  - DoS attacks can be carried out by a number of methods, such as:
    - **Sending a large number of requests to the system:** This can overload the system and make it unavailable to users.
    - **Sending malicious traffic to the system:** This can damage the system or make it unusable.
- **Malware attacks:** Malware can be used to steal data, install backdoors, or disrupt the operation of a cloud-based e-learning system [11].
  - Malware can be spread in a number of ways, such as:
    - **Clicking on a malicious link:** This can download malware onto the user's computer.
    - **Opening an infected attachment:** This can also download malware onto the user's computer.
    - **Using a compromised website:** If a website is compromised, it can be used to spread malware to visitors to the website.
- **Phishing attacks:** Phishing attacks can be used to trick users into revealing their personal information, such as passwords and credit card numbers. This information can then be used to access cloud-based e-learning systems [12]**.**
  - Phishing attacks are often carried out by sending emails or text messages that appear to be from a legitimate source, such as a bank or credit card company. The email or text message will often contain a link that, when clicked, will take the user to a fake website that looks like the real website. Once the user enters their personal information on the fake website, the hacker can steal it.
- **Identity theft:** Identity theft is a serious problem that can occur when a user's personal information is stolen. This information can then be used to open bank accounts, apply for loans, or commit other crimes [13].
  - Identity theft can occur as a result of any of the security breaches or attacks mentioned above. It is important for users to be aware of the risks of identity theft and to take steps to protect themselves, such as using strong passwords and being careful about what information they share online.

These are just some of the digital learning security issues in cloud-based e-learning. By being aware of these risks and taking steps to mitigate them, organisations can help protect their data and prevent security breaches in cloud-based e-learning. Researchers and institutions have been investigating numerous solutions, such as encryption, multi-factor authentication, intrusion detection systems, routine security audits, and continuous monitoring, to address these security concerns. To provide a strong and secure learning environment for higher education institutions, a comprehensive strategy to cloud-based e-learning security combines technical solutions, policy development, and user education.

Overall, these studies show how critical it is for higher education institutions to address security issues related to cloud-based e-learning platforms. To safeguard student data and intellectual property from security risks, institutions must put in place the necessary security measures.

3. Methodology

A preliminary study involves conducting initial research to gather foundational information, insights, and context before embarking on a larger research project. Here's a research methodology for conducting a preliminary study that's shown in Figure 1.

Certainly, let's elaborate on each of these steps in the preliminary study's research methodology:

i. **Define Research Objectives:** In this initial step, clearly outline the specific goals and objectives of the preliminary study. Clarity in the research objectives will guide all subsequent stages of this study.

ii. **Literature Review:** Conduct a thorough review of existing literature related to the research topic. Identify key concepts, theories, methodologies, and findings from relevant academic sources. The literature review helps to understand the current state of knowledge, identify gaps, and contextualize your research within the broader academic discourse.

iii. **Surveys:** Through the use of a structured questionnaire, surveys include gathering quantitative data from a sample of individuals. To make sure that the survey questions are precise, unbiased, and pertinent, match the survey with the study objectives.

iv. **Sampling Strategy:** Choose the population or group to concentrate on. To pick participants from this population, we will select an appropriate sampling approach (convenience, purposeful, random, etc.). Data are guaranteed to be representative of the bigger group according to the sampling procedure.

v. **Data Collection:** Implement survey-based data collection techniques. Administer the questionnaire to the chosen participants, then compile their answers. To preserve data quality and validity, make sure that data gathering is done ethically and consistently.

vi. **Data Analysis:** Use the proper methods to analyze the data that have been gathered. This study summarizes and interprets survey data using descriptive statistics.

vii. **Interpretation and Discussion:** Analyze the conclusions drawn from the data. Talk on the relevance of these findings in light of the study's goals and the larger context. Critical thinking and a thorough comprehension of the data are required for this level.

viii. **Identify Gaps and Further Steps:** Determine any gaps or regions requiring additional research based on an interpretation. This stage establishes the foundation for the remainder of the research and provides guidance for creating the research design.

The goal of a preliminary study is to gather initial insights and lay the groundwork for a larger research endeavour. This methodology is designed to provide a solid foundation for future work and guide the approach toward addressing research gaps and challenges effectively.

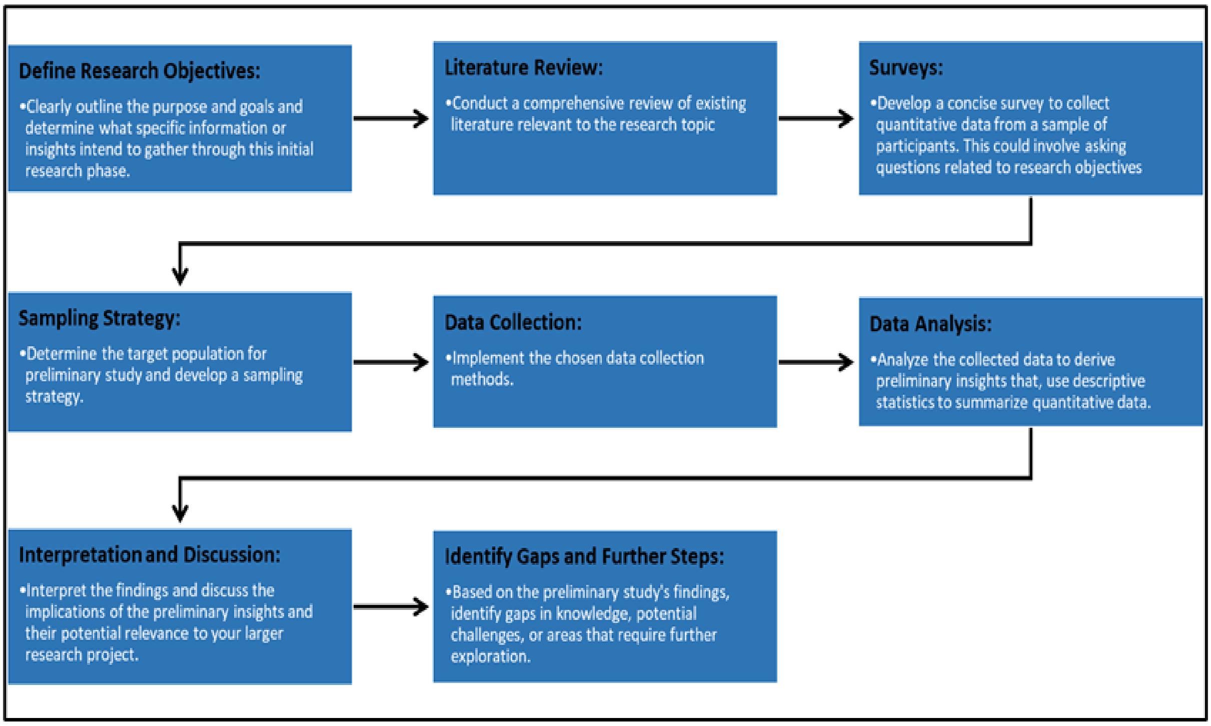
Define Research Objectives:
•Clearly outline the purpose and goals and determine what specific information or insights intend to gather through this initial research phase.
Literature Review:
•Conduct a comprehensive review of existing literature relevant to the research topic
Surveys:
•Develop a concise survey to collect quantitative data from a sample of participants. This could involve asking questions related to research objectives
Sampling Strategy:
•Determine the target population for preliminary study and develop a sampling strategy.
Data Collection:
•Implement the chosen data collection methods.
Data Analysis:
•Analyze the collected data to derive preliminary insights that, use descriptive statistics to summarize quantitative data.
Interpretation and Discussion:
•Interpret the findings and discuss the implications of the preliminary insights and their potential relevance to your larger research project.
Identify Gaps and Further Steps:
•Based on the preliminary study's findings, identify gaps in knowledge, potential challenges, or areas that require further exploration.

Figure 1: The Research Methodology

4. Privacy and Data Protection in E-Learning Based-On Cloud

To adapt the learning process to each individual learner, e-learning systems need to gather information on users. This data contains contact, preference, and relationship details for the student. The gathering, use, disclosure, storage, and destruction of personal data or information that can be used to identify a specific individual are all covered by privacy rights or obligations [12]. Many factors, including nations, cultures, and legal frameworks, have an impact on the idea of privacy. Privacy and data protection are crucial considerations in any e-learning environment. E-learning involves the use of digital technologies to deliver educational materials and activities to students. A few previous studies reviewed to find about security issues in cloud-based e-learning platform as shown in table 1 below.

As a result, sensitive personal and educational data are often collected, stored, and processed by e-learning platforms, which raises concerns about privacy and data protection. Here are some strategies for ensuring data security and privacy in e-learning:

- Use Secure Platforms: Look for an e-learning platform that incorporates encryption and secure data storage while making your choice. Additionally, the platform must abide by pertinent data protection laws including FERPA, the CCPA, and GDPR.
- Obtain Consent: Students must express explicit permission for the use of their academic and personal information in e-learning. A succinct privacy policy that explains how data will be used, who will have access to it, and how it will be protected should be used to gain this consent.
- Limit Data Collection: E-learning platforms should only gather information that is required for the course's delivery. The acquisition of unnecessary data can put students' privacy at danger.
- Provide Data Access: Students should have access to the personal and academic information that e-learning platforms have collected about them. Students can review, edit, and when necessary delete their data thanks to this access.

- Educate Users: Students and instructors should be educated about the importance of privacy and data protection. This education should include best practices for protecting personal and educational data and the potential risks associated with sharing data.

In conclusion, data protection and privacy are crucial factors in e-learning. The emergence and widespread adoption of cloud-based e-learning platforms have introduced a transformative dimension to modern education. While these platforms offer unprecedented flexibility, interactivity, and accessibility, they also raise significant security concerns that necessitate proactive measures to safeguard the privacy and data protection of all stakeholders involved. E-learning platforms can protect students' privacy and personal data by employing secure platforms, gaining informed consent, restricting data collecting, granting data access, and educating users.

Table 1: Summary of Previous Research

Study Title	Research Question	Methodology	Key Findings
"Security Issues and Solutions for E-learning" [15]	What are the major security issues and their solutions in e-learning?	Literature review	Major security issues in e-learning include authentication, authorization, confidentiality, and data integrity. Solutions include encryption, access control, firewalls, and intrusion detection systems.
"Security in Cloud-Based E-Learning: A Systematic Literature Review" [16]	What are the security challenges and solutions in cloud-based e-learning?	Systematic literature review	Security challenges include data breaches, denial of service attacks, and data loss. Solutions include encryption, access control, and intrusion detection systems.
"A Review on Security Issues and Concerns in E-learning" [17]	What are the security issues and concerns in e-learning?	Literature review	Security issues include identity theft, phishing attacks, malware, and social engineering attacks. Concerns include user privacy, data protection, and regulatory compliance.
"Security Issues and Challenges in E-learning: A Review" [18]	What are the security issues and challenges in e-learning?	Literature review	Security issues include authentication, authorization, confidentiality, and data integrity. Challenges include the need for effective security policies, user awareness, and continuous monitoring.
"Cloud Security Issues in E-learning: A Systematic Literature Review" [19]	What is the cloud security issues in e-learning?	Systematic literature review	Cloud security issues include data breaches, insider threats, and denial of service attacks. Solutions include encryption, access control, and intrusion detection systems

5. A Preliminary Study: Result and Discussion

Preliminary studies, also known as feasibility studies, are small-scale research investigations carried out as a first step before beginning a larger research project. Its goal is to collect preliminary information and insights that will aid researchers in determining the viability, technique, and potential difficulties of the larger study. A preliminary study's goal is to serve as a basis for judgments about the research project's general viability, data gathering strategies, and research design. Researchers use preliminary studies to identify relevant variables, relationships, or trends that will guide the development of research hypotheses and objectives. Researchers can improve and modify their study methodologies, instruments, and procedures depending on preliminary studies' findings. By doing this, the primary study is ensured to be well-designed and more likely to produce significant results.

For this research, a preliminary study was conducted in which a questionnaire of eight items was distributed randomly to 122 lecturers in higher education institutions as experts in teaching. There are 67.2% of them who are female, and the rest are male. 95.1% of the respondents stated that their university has an e-learning (LMS) system in their institution. About 87.7% of the respondents stated their HEI allows them to use cloud-based e-learning systems such as Google Classroom, Socrative, Schoology, and open learning, as shown in Figure 2 below. Respondents were also asked about the type of e-learning system that was used in the workplace. Figure 3 below shows the result from the respondents. It found that 44.2% of users use the e-learning system provided by the university only, 3.3% use the e-learning system (a cloud-based System) only, and the rest (52.5%) use both e-Learning and the cloud.

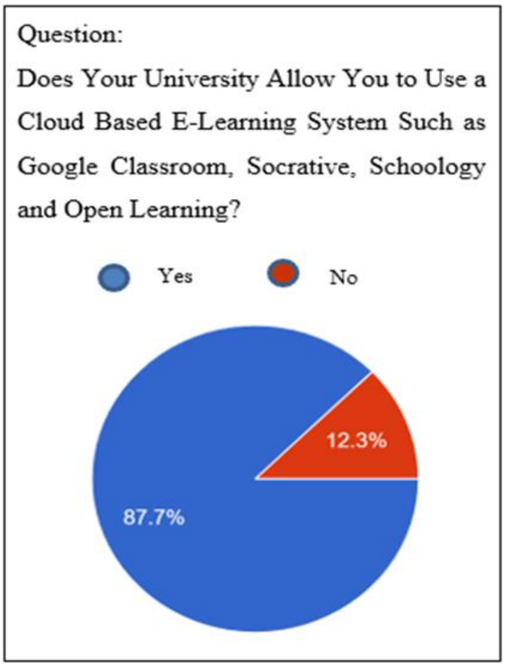

Figure 2: Use of Cloud Based E-Learning in Education

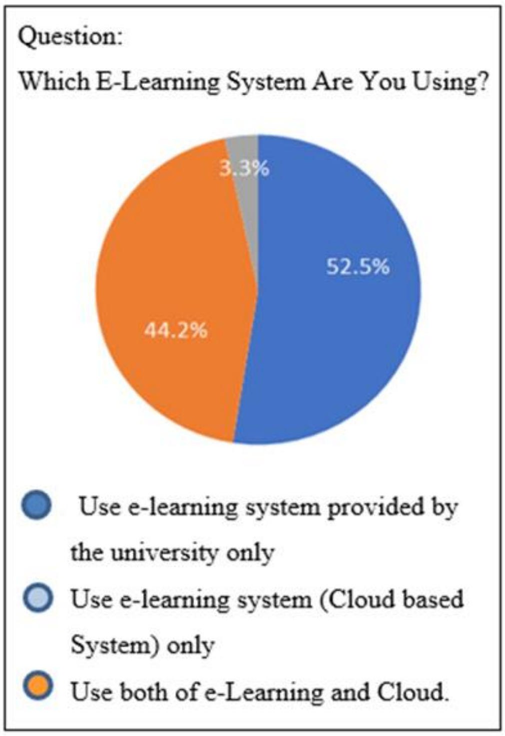

Figure 3: Type of e-Learning Used

Certainly, let's delve deeper into the implications and potential insights that can be drawn from the distribution of user preferences in relation to e-learning systems and cloud-based platforms:

i. **Exclusively University E-Learning System Users (52.5%):** This substantial segment of users shows a clear preference for utilizing the e-learning system provided by the university itself. This could be attributed to various factors, including:

   - **Institutional Trust:** The university's e-learning system is likely well-established and integrated into the academic framework. Users may feel a higher level of trust in the platform's content, security, and overall reliability due to its official status.
   - **Curriculum Alignment:** The university e-learning system might be closely aligned with the academic curriculum, ensuring that students access materials directly related to their courses and subjects.
   - **Accessibility:** Users might find it convenient to access the university's e-learning resources, especially if they are readily available through familiar channels such as the university website or learning management system.

ii. **Exclusively Cloud-Based E-Learning System Users (3.3%):** While a smaller proportion of these users opting solely for a cloud-based e-learning system indicates an interesting trend,

   - **Preference for Specific Features:** This segment could be drawn to the unique features and functionalities offered by the cloud-based e-learning system. These features might include advanced collaboration tools, interactive learning environments, or customizable learning paths that are not available in the university's system.
   - **External Resource Utilization:** Users may have external commitments or learning objectives that align better with the capabilities of the cloud-based platform, prompting them to rely exclusively on it.

iii. **Hybrid Users (44.2%):** The majority of users adopting both the university e-learning system and a cloud-based alternative suggest a nuanced approach to e-learning.

   - **Complementary Benefits:** Users could leverage the strengths of each system. For instance, they may utilize the university's platform for core coursework and official resources while turning to the cloud-based system for supplementary materials, interactive exercises, or collaborative projects.
   - **Flexibility and Diversity:** This segment values the flexibility to choose the most suitable platform for different learning scenarios. They might switch between the systems based on specific needs, enhancing their learning experience.
   - **Adaptation to Varied Learning Styles:** The use of both systems may cater to diverse learning preferences and styles. Some users might find certain subjects or concepts better explained on one platform versus the other.

Overall, this distribution highlights the multifaceted nature of modern e-learning practices. It underscores the importance of offering a range of e-learning solutions to accommodate various learning preferences and needs. Institutions should consider these findings when designing and implementing their e-learning strategies, aiming to provide a seamless and enriching learning experience for all users. Additionally, ongoing research and analysis could uncover deeper insights into the factors driving these preferences and inform strategies to further optimize e-learning ecosystems.

Respondents were also asked about the main factors that encourage the use of the cloud system. Among the factors are the easy-to-access factor, the functions provided on that platform, the trust factor, the technical support factor, the intention factor, the HEI Policy factor, and the social influence factor. Referring to figure 4 below, the highest influence factors that encourage lecturers to use cloud-based learning platforms are the trust factor (73.1%), secondly, the technical support provided in that platform (63.4%), followed by easy access (40.9%), then HEI policy (37.6%), and then the fifth factor is an intention factor (36.6%). The third last factor is function provided in a cloud-based system (33.3%), followed by social influence (18.3%), and the last factor is others (4.4%). This finding shows that most lecturers use cloud-based systems due to three main factors: trust, technical support provided, and easy access. All the factors mentioned are strongly related to the threat of data security issues.

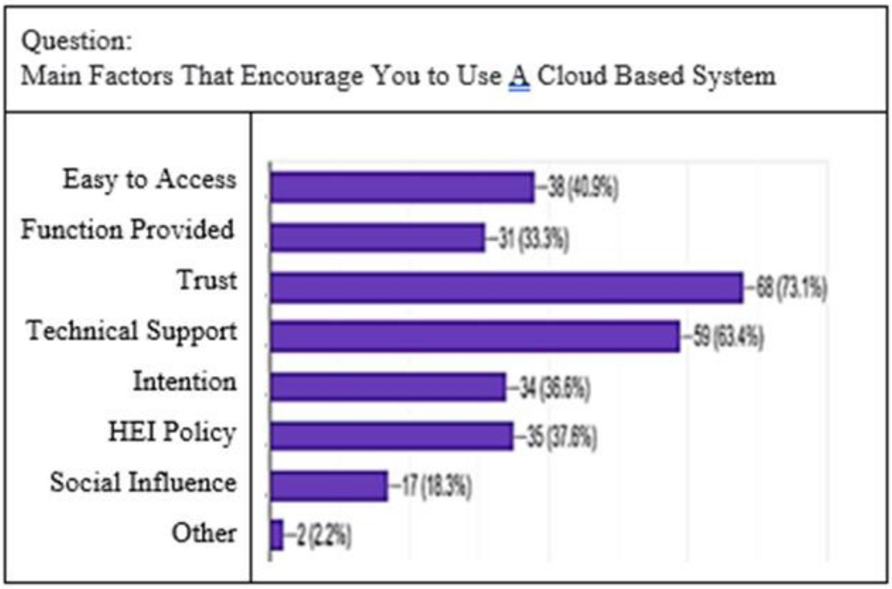

Figure 4: Factors to use Cloud Based System

The provided data outlines the key factors influencing lecturers' adoption of cloud-based learning platforms and emphasizes their significance within the context of data security concerns. Let's delve into a more detailed elaboration of these findings:

i. **Trust (73.1%)**: Most respondents expressed a high level of trust in cloud-based systems, suggesting that they believe these systems are reliable and secure.

ii. **Technical Support (63.4%)**: A significant portion of respondents value the availability of technical support, indicating that having assistance and guidance plays a crucial role in their decision to use a cloud-based system.

iii. **Easy Access (40.9%)**: While slightly lower than trust and technical support, easy accessibility remains a prominent factor, showing that users appreciate the convenience of accessing resources and data anytime, anywhere.

iv. **Functionality Provided (33.3%)**: Functionality is another important consideration, with over a third of respondents valuing the features and capabilities offered by the cloud-based system.

v. **HEI Policy (37.8%)**: Higher Education Institution (HEI) policies also play a notable role, indicating that organizational guidelines and regulations influence the choice of cloud-based systems.

vi. **Intention (36.6%)**: Respondents seem to have a degree of intention or motivation to use these systems, though it is not as dominant a factor as trust or technical support.

vii. **Social Influence (18.3%)**: Social factors, such as recommendations from peers or colleagues, have a relatively lower impact on the decision to adopt cloud-based systems, according to this survey.

viii. **Other Factors (2.2%)**: A small percentage falls under "other" factors, which may include specific, unique considerations that are not explicitly mentioned in the survey.

Overall, trust, technical support, and easy access appear to be the primary driving factors behind the adoption of cloud-based systems in this survey. These findings suggest that users prioritize reliability, assistance, and convenience when selecting such systems for their needs.

6. Conclusion and Further Research

Result from the preliminary study that the respondents gave about the main factors that encourage the use of the cloud system provided by the university. Based on the findings, we found that the majority of academicians in higher education use cloud-based learning platforms due to various factors that encourage them to do so. This scenario will be faced with cloud-based e-Learning security issues.

The extensive use of cloud technology in the educational domain has led to the recognition of the critical need for a comprehensive and adaptable Digital Learning Security Model. The data collected from our preliminary study has unveiled a multifaceted landscape of motivations driving educators' use of cloud-based e-learning systems. It is evident that practicality, functionality, trustworthiness, and support are pivotal factors influencing the adoption of these platforms. However, amid these motivators lies a persistent concern: the security of sensitive data. Educators and institutions alike are acutely aware of the potential vulnerabilities that accompany the integration of cloud-based technologies, particularly regarding unauthorized access, data breaches, and privacy infringements.

The need for a Digital Learning Security Model is underscored by several key considerations:

i. **Mitigating Security Threats:** The diverse motivations of educators converge on the fundamental necessity of addressing security threats effectively. A well-structured security model can counteract potential risks, ensuring that educators can engage confidently in e-learning activities without compromising the safety of their data.

ii. **Balancing Usability and Security:** The model should strike a delicate balance between robust security measures and user-friendly functionality. It must offer seamless integration with e-learning platforms while upholding stringent privacy and data protection protocols.

iii. **Customization and Adaptability:** Recognizing the dynamic nature of technology, the security model should be adaptable to various e-learning environments, catering to the unique needs of different institutions, educators, and learners. Customizable security solutions can ensure a tailored approach to data protection.

iv. **Fostering Trust and Compliance:** Trust is paramount in the digital realm. The security model should in still confidence in educators, learners, and institutions by adhering to best practices, legal frameworks, and industry standards for data privacy and security.

v. **Enhancing Educational Ecosystems:** By bolstering security and data protection, the model contributes to an enhanced educational ecosystem where educators can harness the full potential of cloud-based e-learning platforms, creating immersive and enriching learning experiences.

In essence, the imperative to develop a Digital Learning Security Model arises from a collective commitment to advancing educational technology while safeguarding the sensitive information that underpins modern pedagogy. The model, designed with an intrinsic understanding of educators' motivations and security concerns, will serve as a cornerstone for fostering secure, innovative, and effective e-learning environments. It represents a proactive step toward harmonizing the powerful benefits of cloud-based e-learning with the paramount importance of privacy and data protection, ultimately shaping a more resilient and responsible digital educational landscape for the future.

In summary, the insights gleaned from the data underscore the importance of developing a Digital Learning Security Model as our future work that aligns with the motivations and usage patterns of educators. By catering to practicality, functionality, trustworthiness, and support while also accommodating the evolving landscape of e-learning platforms, this model can effectively enhance e-learning privacy and data protection, ultimately creating a secure and conducive digital learning environment. Findings from the literature review show a few security issues highlighted and challenges as well, which motivate future work by providing a comprehensive digital learning security model for addressing privacy and data protection concerns in e-learning environments, which exposes students and institutions to potential cyber threats and compromises their privacy and data security.

References

[1] A. Yacob, Z. Baharum, W. M. A. F. W. Hamzah, A. Z. A. Kadir, N. S. Sulaiman, and Nur Sukinah Aziz, "The World of Digital Education : A Solution for Today ' s Challenges ?," *5th Int. Conference Eng. Technology*, vol. 4, no. 1, pp. 1–10, 2021.

[2] A. Yacob, A. Z. A. Kadir, O. Zainudin, and A. Zurairah, "Student Awareness Towards E-Learning In Education," *Procedia - Soc. Behav. Sci.*, vol. 67, no. November 2011, pp. 93–101, 2012, doi: 10.1016/j.sbspro.2012.11.310.

[3] A. Yacob, Z. Baharum, N. Aziz, N. S. Sulaiman, and W. M. A. F. W. Hamzah, "A review of internet of things (IoT): Implementations and challenges," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1 Special Issue 3, pp. 373–376, 2020, doi: 10.30534/ijatcse/2020/5891.32020.

[4] N. S. Sulaiman *et al.*, "A Review of Cyber Security Awareness (CSA) Among Young Generation: Issue and Countermeasure," *Lect. Notes Networks Syst.*, vol. 322, no. January, pp. 957–967, 2022, doi: 10.1007/978-3-030-85990-9_76.

[5] N. S. Sulaiman, N. S. Aziz, and A. Nasir, "Cyber Security Awareness Model (Among Children) Using Protection Motivation Theory : A Review," vol. 5, pp. 74–85, 2023.

[6**]** Gupta, I., Singh, N., & Singh, A.K. (2019). Layer-based Privacy and Security Architecture for Cloud Data Sharing. *Journal of Communications Software and Systems*.

[7] Karmakar, A., Raghuthaman, A., Kote, O.S and Jayapandian, N. (2022) "Cloud Computing Application: Research Challenges and Opportunity," *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Erode, India, 2022, pp. 1284-1289

[8] Alenezi, A., Atlam, H.F. & Wills, G.B. (2019) Experts reviews of a cloud forensic readiness framework for organizations. *J Cloud Comp* **8**, 11

[9] Hyungjin, L. K., Hovav, A., & Han, J. (2020). Protecting intellectual property from insider threats: A management information security intelligence perspective. *Journal of Intellectual Capital*, *21*(2), 181-202

[10] Manimaran, A., & Durairaj, M. (2013). A study on security issues in cloud based e-learning. School of Computer Science Engineering & Applications, Bharathidasan University, Trichy-620023, India.

[11] Kumar, G. (2011). Security issues in cloud based e-learning. Master's thesis, University of Boras, Sweden.

[12] Ishita Banik (2023). The Importance of Security in eLearning Platforms. https://www.muvi.com/blogs/the-importance-of-security-in-elearning-platforms Access date: August 2023

[13] Durairaj, M., & Manimaran, A. (2015). A study on security issues in cloud based e-learning. *Indian Journal of Science and Technology*, *8*(8), 757-765.

[14] Ahmed, M., & Sarkar, N. I. (2021). Privacy in Cloud- Based Computing. *Research Anthology on Privatizing and Securing Data*, 154–168.

[15] Kaur, H., & Singh, H. (2018). Security Issues and Solutions for E-learning. International Journal of Innovative Research in Computer and Communication Engineering, 6(5), 5108-5114.

[16] Yousuf, M. A., & Hassan, S. A. (2018). Security in Cloud-Based E-Learning: A Systematic Literature Review. International Journal of Computer Science and Network Security, 18(6), 83-90.

[17] Suresh, P. R., & Jayanthi, D. (2019). A Review on Security Issues and Concerns in E-learning. International Journal of Recent Technology and Engineering, 7(6), 343-348.

[18] Saravanakumar, R., & Asokan, V. (2019). Security Issues and Challenges in E-learning: A Review. Journal of Critical Reviews, 6(7), 527-532.

[19] Ali, M., El-Alfy, E. S., Abdelfatah, M. A., & Hassanien, A. E. (2021). Cloud Security Issues in E-learning: A Systematic Literature Review. Journal of King Saud University-Computer and Information Sciences, 33(1), 62-72.