International Journal of Natural & Applied Science
Volume 5, Number 1, March 2024
http://www.cedtechjournals.org
ISSN: 2756-4606

MOBILE LEARNING SYSTEM: ATTACK ISSUES, CONTROL MEASURES AND RECOMMENDATION

***Adamu, M., Oyefolahan, O. I., Ojerinde, O. A**
*Department of Computer Science, Federal Polytechnic, P.M.B. 55, Bida, Niger
[2]Department of Information Technology, Federal University of Technology, Minna, Niger
[3]Department of Computer Science, Federal University of Technology, Minna, Niger
Email: bejian2004@gmail.com

ABSTRACT

Despite the existence of some literature reviews on the security issues tied to mobile devices in education, they fall short of thoroughly exploring the security challenges inherent in mobile learning systems. This study sets out to bridge this gap by investigating the security challenges faced by mobile learning, organizing them according to the specific security needs and vulnerabilities inherent to mobile learning, and spotlighting preventive strategies along with recent findings in the realm of mobile learning security. To meet its research goals, the study employed a systematic literature review method guided by the PRISMA approach, establishing quality standards that reflect the study's aims, undertaken tasks, and the knowledge base relevant to the security challenges of mobile learning systems. This analysis encompasses studies published from 2012 to 2022, focusing on "mobile learning," "mobile education," "security challenge," and "security trend" as key search terms. It sourced articles from a variety of databases, including Google Search, IEEE, WILEY, Scopus, ACM Digital Library, Science Direct, and Springer, initially identifying 116 relevant articles. Strict criteria were applied, narrowing down to 46 articles for detailed examination. The findings reveal a significant gap in the literature on security challenges within mobile learning systems, underscoring the urgent need to address these issues in the rapidly evolving tech landscape. Most existing studies lack a holistic framework for tackling security concerns in mobile learning. Consequently, this paper enriches the existing knowledge for users of mobile learning, students engaged in mobile learning, and the research community focused on the current security challenges posed by the advent of mobile learning.

Keywords: *Mobile Learning, M-learning, Mobile Devices, and Security Challenges*

INTRODUCTION

Mobile technology has played a crucial role in helping humanity by providing an important means of interaction in the social world as well as in teaching and learning. The mobile learning system (M-Learning) seems to be a very necessary tool for students. It can help you get learning materials, knowledge and information anytime and anywhere in your daily life. The massive use of mobile devices such as headphones, iPads, smartphones, tablets and PDAs is an international phenomenon. has provided significant support in various areas such as school, university and education system [1]. Mobile learning is an educational approach that leverages mobile devices and includes four main elements: input, discovery, output and connectivity. It allows students to learn anywhere, anytime outside of traditional classroom environments, making it easier to integrate their learning experiences. [2]. Mobile learning is becoming increasingly popular because it offers solutions to specific educational challenges, complements and expands formal education, supports students of all ages and socioeconomic backgrounds, and provides educational opportunities in areas where they would otherwise be scarce. [3]. The development of mobile technologies, including mobile devices and wireless networks, has played an important role in improving the education sector through the emergence of mobile learning (m-learning). These mobile learning platforms are designed to complement advances in mobile technology and make education accessible, more interactive and adaptable everywhere. [4]. Mobile learning is a learning method that involves sharing and distributing information. It can be used as an alternative to traditional classroom activities for students who may not be able to participate in traditional classroom activities (Khan et al., 2019). M-Learning is largely supported by the convergence of the Internet and information technologies into a single entity called the Internet of Things [4]. The mobile learning system uses the Internet to exchange and distribute data and information.

However, advances in mobile technology have placed mobile learning at the forefront of security threats. Individuals, organizations, and developers pay little attention to security issues in mobile learning, and security is a pressing and often overlooked issue. [5]. The Internet (wireless network) as the backbone of the mobile learning system is not secure, and the uncertainty inherited from the wireless network may be transferred to the mobile learning system (Khan et al., 2019).

M-Learning systems contain a lot of very personal and professional data that is very confidential and therefore must be protected from misuse and unauthorized access. Security issues in a mobile learning environment are very important and should be taken into account by ensuring that information security countermeasures are implemented in mobile learning. Examples of business-critical data that is highly sensitive information include course materials, assignment submissions, exam question results, and quizzes [6].

Security aspects of m-learning include protection against manipulation (e.g. by a student or intern), user authentication and data protection. As mobile learning capabilities increase, information must be actively protected to avoid loss of confidentiality, availability and integrity. Information security is very important; Therefore, confidential information should be limited to a few well-defined groups. Examples of sensitive academic information include course materials for specific groups, electronic outcomes for specific individuals, and copyright protection of intellectual property [7].

In addition, vulnerabilities (limited power, insufficient storage, low processing power) of mobile devices can be transferred to the m-learning system, making it easier for attackers to disclose, modify and steal sensitive academic information without the consent of teachers or owners. Since this is not the case, it is possible to apply a strict security approach to mobile devices, which are the main tool of the mobile learning system (Dhanda et al., 2020). Mobile devices use wireless communication methods and are designed for open use, which exposes them to security risks. Due to the nature of wireless transmission, information can easily be intercepted and altered. Given the essential services these devices provide, protecting information is critical as tampering or interception can result in data loss. Mobile devices face numerous security challenges, including software-related threats such as viruses, denial-of-service attacks, and macro worms; hardware problems such as theft and espionage; and intellectual property violations, including copyright infringement and piracy (Dhanda et al., 2020). The widespread, maneuverability, and portability of mobile devices make them vulnerable to software, hardware, and cyber-attacks. Security threats in mobile learning systems seem to be increasing quite rapidly among teachers, especially in developing countries like Nigeria where cybercrime, fraud, theft, copyright and cyber security threats are rampant [4]. Therefore, it is important to review the existing mobile learning security challenges to present the current status of security challenges and

help mobile learning stakeholders implement a safe and reliable mobile learning security system. The study makes a three-part contribution. First, existing security issues are identified and classified based on the security requirements and vulnerabilities specific to mobile learning systems. Preventative strategies to address these safety issues in mobile learning environments are then outlined and areas for future research are suggested. The structure of the article is as follows: In the second section, studies and analyzes on the topic of security in mobile learning are discussed. The third section of this introduces a comprehensive taxonomy of criteria relevant to mobile learning security. This is followed in the fourth section by a detailed discussion of literature classification and research. The fifth section addresses open questions within the study, while the sixth section describes possible approaches for future research. Concluding remarks can be found in the seventh section.

LITERATURE REVIEW

There has been little research recently in the area of security challenges or risks in mobile learning. This literature does not adequately describe the security challenges in mobile learning. Previously published reviews in this area are summarized in Table 1. This section of the study reviews related literature works to identify their shortcomings in order to highlight them difference from this study as presented in Table 1.

Table 1: Previous Review Papers

Reference	Latest Reference	Methodology	Strength	Limitation
Kamborakis(2013)	2012	Review	System and data security and privacy, user privacy, mobile device related issue, content filtering, content copyright and intellectual property right etc.	Vulnerability issues of mobile learning are lacking in the study.
Khan (2015)	2014	Survey	Threats from physical sources, threats from applications, threats related to networks, threats related to web usage, and issues related to vulnerabilities.	Based on user's data privacy and biometric approach may not be suitable for mobile devices
Adetoba *et al.* (2016)	2015	Review	Confidentiality attacks, integrity attacks, availability attacks, authentication attacks, and authorization attacks.	Based on security challenges to the e-learning system
Mkpojiosu *et al.* (2019)	2018	Systematic Literature Review	Confidentiality attack, integrity attack, reliability attack, trust, privacy and availability of information	Vulnerability issue, copyright threat and the use of lightweight cryptography primitives are not included in the work
\Qamar *et al.*, (2019)	2018	Review	Malware attacks such Virus, Worm, Trojan, Spyware, Adware, Ransomware, Root Exploit, Backdoors, and Keylogger's	Based on mobile malware attacks
Tao *et al.*, (2020)	2019	Review	Privacy-violating threats, malicious attacks (high energy consumption), bug (system crash), and ransom ware and spam	Suggestions or recommendations on security control measures is lacking in the study
Saikatet *et al*., (2021)	2020	Systematic Literature Review	Security and privacy concern, data security, and offline access to material and assessment is cumbersome for widespread usage	Lacking of comprehensive discussion on security issues confronting mobile learning adoption.
Nikhil *et al*., (2021)	2019	Survey	Cross site scripting assaults, content assaults, cross-site request forgery assaults, SQL injection attack, session hijacking, DDoS attack, and Man in Middle attack.	Based on survey study.
Sapanca & Kanbul (2022)	2022	Survey	Confidentiality, Availability, and integrity attacks on information system	A survey study
Present review	2023	Systematic Literature Review	Confidentiality attack, integrity attack, availability attack, authentication attack, non-repudiation attacks, and vulnerability issues	Based on the three major components of mobile learning system (mobile device, database server, and network) security issues.

Based on the limitations of the previously reviewed articles as shown in Table 1, the proposed study reviewed the existing literature on security challenges in mobile learning from 2012 to 2022 to provide a more comprehensive literature to fill and update the gaps.

Research Methodology

The analysis sheds light on unexplored areas concerning the security challenges faced by mobile learning systems designed to cater to student preferences. Despite considerable research focused on security threats to mobile learning, there remains a notable deficiency in adequately pinpointing the security issues within mobile learning systems. This examination of the prevailing security threats to mobile learning was undertaken utilizing the PRISMA method. The review process is divided into two stages: initially, the review is conducted, considering data sources, search terms, quality evaluations, and criteria for inclusion and exclusion, which is then followed by reporting the study and documenting the findings.

Conducting the Review

The purpose of this study is to examine the security challenges of mobile learning. A literature review is one way to gain knowledge in this area and to assess the scope of research activities related to security challenges in mobile learning.

Search Strategy

The search strategy aims to identify the most relevant and up-to-date studies on security issues in mobile learning while managing the volume of reviewed publications. Google Scholar stands out as the most comprehensive academic search engine because it can index articles from a wide range of academic publishers and professional associations. To ensure a comprehensive literature search, keyword searches were also conducted in several recognized databases, including Science Direct, ACM Digital Library, IEEE Xplore, Scopus, and Wiley. The databases were searched for relevant materials using advanced search functions and an extensive keyword list. The search formula used was: (Mobile Learning) OR (M-Learning) OR (Mobile Device) OR (Security Challenges) OR (Security Threats) OR (Security Issues). As mentioned earlier, several databases were used for this research. A total of 117 articles were identified from the collective databases, of which

were selected for inclusion in the study. Table 2 shows the different databases consulted and the total number of articles selected from each database.

Table 2: Database and Selected Articles

Database	Articles found	Relevant Articles	Most Relevant Articles
Google Scholar	74	44	30
Science Direct	25	12	13
IEEE Explorer	9	6	3
ACM Digital	3	3	-
Scopus	3	3	-
Wiley	2	2	-
Total	117	71	46

Inclusion and exclusion criteria

The inclusion and exclusion criteria are used to filter the published articles related to mobile learning security threats

Inclusion criteria:

- Articles spanning from 2012 to 2022.
- Papers focused on learning management systems.
- Articles that discuss the benefits and obstacles of mobile learning, along with an overview and analysis of current mobile learning **systems.**
- Articles focused on security issues related to mobile learning, including reviews and ratings of current mobile learning platforms.
- The articles underwent peer review.
- Complete article available in English

Exclusion criteria:

- Articles that detail systems that do not provide original research, such as those addressing security challenges in mobile learning systems.
- The mobile device should not include laptops or netbooks.
- Articles outside the 2012 to 2022 timeframe

Quality Assessment

Quality assessment is carried out on pre-selected studies after reviewing them against inclusion and exclusion criteria to ensure that they meet the study quality standards. The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) approach was used to define quality criteria, focusing on the research objectives, hypotheses and relevant knowledge related to the study of security challenges in mobile learning (Moher et al., 2015). The following questions are used as a checklist to measure the research credibility and validity:

- Does the research improve our understanding of security issues in mobile learning?
- Do the study results provide reliable and accurate information on security issues in mobile learning?
- Are the goals and objectives of the research clearly defined to effectively contribute to the knowledge base on security issues in mobile learning?

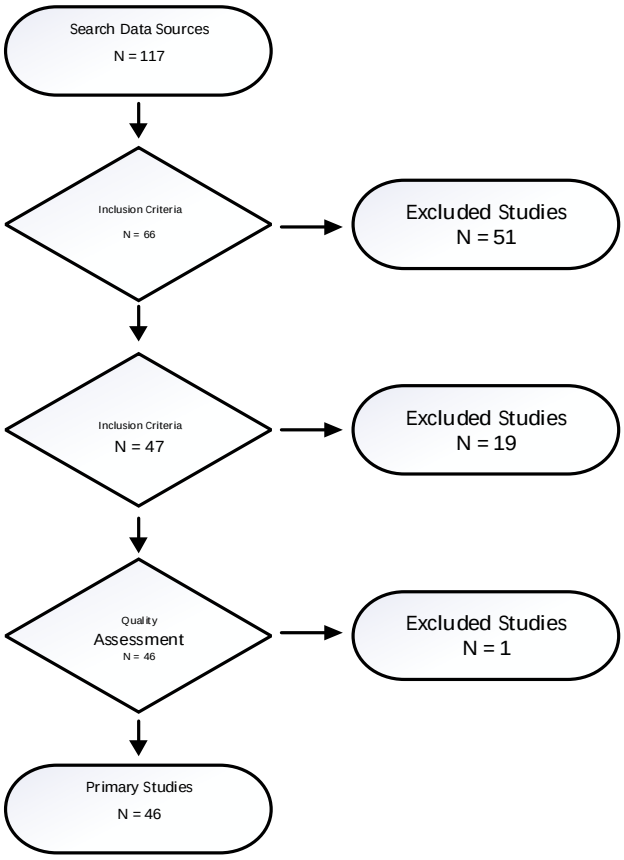

Figure1: PRISMA flowchart

Since all the quality assessment criteria are important in the context of the research questions, only 46 studies had been selected for the final review (Fig. 1)

Security Attacks and Vulnerabilities in Mobile Learning System.

Mobile learning system encounters a lot of security attacks and vulnerability issues inherited from the mobile devices which are the principal tool used in the mobile learning environment. The vulnerability issues and attacks are attributed to limited resources of the same devices and the use of wireless network that is open channel which give rooms for attackers to easily penetrate the system. Table 3 presents the existing attacks and vulnerability issues in mobile learning system.

Table 3: Security Attacks and Vulnerabilities in Mobile Learning System

Author(s)/Year of Publication	A	B	C	D	E	F
Sexena & Chaudhari (2012)	√	√	√	√		
Kambourakis (2013)	√	√	√			
Dewan & Chaudhury (2013)	√	√	√	√		
Shonola & Joy (2014a)	√	√	√	√		√
Shonola & Joy (2014b)	√	√	√	√		√
Zouka (2015)	√	√	√	√		√
Khan et al. (2015)	√			√		
Belhaj & Samir (2015)	√	√		√		
Study (2015)	√	√				√
Diana et al. (2015)	√	√	√	√		√
Mohsen et al. (2016)	√	√	√		√	√
Adeotoba et al. (2016)	√	√	√	√		√
Kambourakis (2016)	√	√	√			√
Mubuke et al. (2016)	√		√	√		√
Sadeqhzadeh & Nakhaei (2017)	√	√	√			
Vorakulpitat et al. (2017)	√	√	√	√		√
Singh et al. (2017)	√		√	√		√
Cheng et al. (2017)	√	√	√			
Manmeet et al. (2017)	√	√	√	√		
Kim et al (2017)	√			√		√
Ochaya (2018)	√	√				√
Mathematics et al. (2018)	√	√	√			
Al-humumaiyyan et al. (2018)	√			√		
Balamurugan et al. (2018)	√	√		√		
Elsand (2018)	√	√	√		√	
Battle (2018)	√		√	√		√
Abawajy (2018)	√		√			
Mseteka & Phiri (2019)	√	√	√			
Kumar et al. (2019)	√	√	√	√		
Khan et al. (2019)	√	√		√		√
Ibrahim et al. (2019)				√		√
Bhat & Dutta (2019)	√	√	√	√		√
Mkpojiosu et al. (2019)	√	√	√	√		
Dhanda et al. (2020)	√	√				
Wang et al. (2020)	√			√		
Litoussi et al (2020)	√	√	√	√		√
Tao et al. (2020)	√	√	√	√		

Yaacoub et al. (2020)	√	√	√		√	
Nikhil et al. (2021)	√	√	√	√		√
Korac & Dantanovi (2021)	√	√				√
Sophonhiranrak (2021)	√	√	√	√		√
Sletten et al. (2021)	√		√		√	
Garg & Baliyan (2021)	√	√	√	√		√
Saikat et al. (2021)	√	√	√	√		
Criollo-c et al. (2021)	√					
Sapanca & Kanbul (2022)	√	√	√			

A: Confidentiality attack; **B**: Integrity attack; **C**: Availability attack; **D**: Authentication attack; **E**: Non-Repudiation attack: **F**: Vulnerability issues.

Confidentiality attack: An attack that leak confidential information or data to unauthorized users. **Integrity attack**: An attack that changes the contents of the system. **Availability attack**: An attack that denies the services of a system and contents to be available to legitimate users for a period of time.

Authentication attack.: An attack that uses forge passwords to gain access to the system information. **Non-repudiation attack**: An attack that denies the source of information.

Vulnerability attack: A digital attack that penetrate mobile devices due to the weakness in the development process of mobile software or service.

Control Measures

Based on a literature review on this topic, it has been clearly established that security challenges exist in mobile applications and that threats related to confidentiality, integrity and availability are the most common attacks on mobile and IoT applications, which is a proven security problem. It remains an open controversy and there is no adequate solution.

The following are some control measures;

- The first task in alleviating security issues in m- learning is to create awareness and educate m-learning stakeholders about security threats
- M-learning stakeholders especially the learners should avoid the

use of unsecure network (free available Wi-Fi).

- Use of robust access control mechanisms for authentication and authorization before permission is given to access the device or view learning content and materials,
- Devices like mobile or smartphones should remain in owners' pockets when not in use while tablets should be kept away,
- Mobile learning sensitive data or information such lecture notes for certain individual or group, assessment records, grades, and intellectual properties should be encrypted to prevent from unauthorized access and alteration during storage and transmission,
- To develop mobile devices with enhanced OS to overcomes the loopholes on open source operating system (software component) which make mobile device susceptible to attacks,
- To develop mobile devices with rich resources (memory, battery and processor) so as to enforce stronger security solution.

CONCLUSION

Mobile learning offers a lot of opportunities for the expansion of education and learning beyond the classroom, particularly, in developing countries. The advances in mobile technologies have placed mobile learning in the frontline of security attacks and often neglected. It is established there exist security challenges with the emphases on confidentiality, integrity, and availability attacks of mobile learning system from the reviewed of various related literature works on security challenges confronting m-learning and the study provides preventive measures as it is of utmost importance that the security issues are addressed.

RECOMMENDATION

Many individuals, organizations and developers neglect security issues. As mobile learning is expanding, the security threats is growing and there is the need for individuals, organizations and developers to enhance on security requirements of mobile learning system especially on the basic security traits which are confidentiality, integrity, and availability. The security challenge of mobile learning is a burning issue and often neglected.

- The need to classify the security challenges encounters in mobile into the basic components of a mobile learning system

which are mobile device, server, and network infrastructure for better understanding of the security issue.

- The use of lightweight cryptography techniques for encryption of mobile learning sensitive materials as mobile devices are subjected to limited power supply, low memory capacity and low computational power,
- The use of hybrid lightweight cryptography techniques is recommended as single techniques may not provide optimal solution because of limitations associated with each encryption algorithm being Symmetric or Asymmetric, and
- The use of dynamic encryption techniques to overcomes the limitation of static encryption techniques in which some advance malware such as brute force attack can use try and error to guess the private key.
- Also, the need to develop a robust dynamic randomize AES cryptography model to address the security threats to ensure mobile learning system becomes secure and reliable and meeting the resources ultilazation.

REFERENCES

[1] T. Dhara and S. Bandyopadhyay, "Mobile learning: It's factors and challenges: A literature review," *3*(1), pp. 210–213, 2021

[2] S. Sophonhiranrak, "Features, barriers, and influencing factors of mobile learning in higher education: A systematic review," *Heliyon*, vol. 7, October 2020, e06696

[3] L. Mseteka and J. Phiri, "A Secure Model for Storage and Dissemination of Examination Results: A Case Study of Zambia Technical Education Vocational and Entrepreneurship Training Authority," *Journal of Computer Science*, vol. 15, no. 2, pp. 221–234, 2019

[4] S. S. Oyelere and Y. M. Malgwi, "Cybersecurity Issues on Web-Based Systems in Nigeria: M-Learning Case Study," November, 2015

[5] N. Pinnamaneni, S. C. Muvva, and S. Dodda, "A Study on Threats to Mobile-Learning," *EPRA International Journal of Research & Development (IJRD)*, vol. 7838, July, pp. 271–279, 2021

[6] A. Mathematics, A. Uniyal, P. Kumar, and N. S. Panwar, "Enhanced USB-Token based Secure Authentication Scheme for M-Learning Applications," *119*(12), pp. 12603–12609, 2018.

[7] T. Adetoba and S. Kuyoro, "E-learning security issues and challenges: A review," *Computer Science, Education*, 2016

[8] G. Kambourakis, "Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art," *International Journal of U- & E-Service, Science & Technology*, *6*(3), pp. 67–84, 2013.

[9] C. Tao, H. Guo, Z. Huang, "Identifying security issues for mobile applications based on user review summarization," *Information and Software Technology*, vol. 122, February, 106290, 2020.

[10] S. Saikat, J. S. Dhillon, W. Fatimah, W. Ahmad, and R. A. Jamaluddin, "A Systematic Review of the Benefits and Challenges of Mobile Learning during the COVID-19 Pandemic," *education sciences*

[11] S. Criollo-C, A. Guerrero-Arias, A. Jaramillo-Alcázar, and S. Luján-Mora, "Mobile Learning Technologies for Education: Benefits and Pending Issues," *Applied Sciences*, vol. 11, no. 9, p. 4111, 2021 .

[12] Sapanca and Kanbul, "Risk Management in Digitalized Educational Environments: Teacher's Information Security Awareness Levels," 2022

[13] N. Saxena and N. S. Chaudhari, "A secure approach for SMS in GSM network," in *ACM International Conference Proceeding Series*, pp. 59–64, 2012

[14] J. Dewan and M. Chowdhury, "A Framework for Mobile eLearning (mLearning) with Content Security and Authentication," in *IEEE 2013 Second IIAI International Conference on Advanced Applied Informatics*, pp. 95–99, 2013

[15] S. A. Shonola, M. Joy, "Security Framework for Mobile learning environments," in *7th International Conference of Education, Research and Innovation Conference*, November, pp. 3333–3342, 2014

[16] S. A. Shonola, M. S. Joy, "Investigating Attack Vectors in M-learning Systems in Nigerian Universities," pp. 178–184, 2014

[17] F. Diana, S. Bahry, N. Anwar, N. Amran, and R. P. Mohd, "Conceptualizing security measures on mobile learning for Malaysian higher education institutions," *176*, pp. 1083–1088, 2015

[18] G. Kambourakis, "Security and privacy in m-learning and beyond: Challenges and state-of-the-art," *Computer Science, Education*, January 2016 .

[19] S. H. Sadeghzadeh and A. Nakhaei, "Proposing a Secure Architecture for Mobile-Learning Environments and Investigating

Teachers' Attitude," *Interdisciplinary Journal of Virtual Learning in Medical Sciences*, vol. 8, no. 3, pp. 1–8, 2017.

[20] C. Vorakulpipat, S. Sirapaisan, E. Rattanalerdnusorn, V. Savangsuk, "A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives," *Security and Communication Networks (WILEY)*, vol. 2017, Article ID 2057260, 11 pages.

[21] M. M. Singh, C. W. Chan, Z. Zulkefli, "Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm," *International Journal of Advanced Computer Science*, vol. 8, no. 2, pp. 53–6, 2017.

[22] L. Cheng, F. Liu, and D. D. Yao, "Enterprise data breach: causes, challenges, prevention, and future," 2017.

[23] G. L. Kim, J. D. Lim, and J. N. Kim, "Mobile security solution for sensitive data leakage prevention," *ACM International Conference Proceeding Series*, Part F128004, pp. 59–64, 2017.

[24] W. Ochaya, "The Cyberthreat in IoT, Mobile Learning, and Wearable Devices in Education," 1, pp. 1–18, 2018.

[25] A. Al-Hunaiyyan, R. A. Alhajri, and S. Al-Sharhan, "Perceptions and challenges of mobile learning in Kuwait," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 2, pp. 279–289, 2018.

[26] W. K. Elsand, "Securing Sensitive Digital Data in Educational Institutions using Encryption Technology," *International Journal of Computer Science and Information Security*, *16*(6), pp. 1–8, 2018.

[27] K. Battle, "Security Management for Mobile Devices of Higher Education," *Spring. Mathematics and Computer Science Capstone, La Salle University*, 2018.

[28] J. Abawajy, S. Huda, S. Sharmeen, M. M. Hassan, and A. Almogren, "Identifying cyber threats to mobile-IoT applications in edge computing paradigm," *Future Generation Computer Systems*, vol. 89, pp. 525–538, 2018.

[29] S. Aljawarneh, V. Radhakrishna, and G. R. Kumar, "A recent survey on challenges in security and privacy in internet of things," in *ACM International Conference Proceeding Series*, pp. 1–9, 2019.

[30] P. Bhat and K. Dutta, "A survey on various threats and current state of security in android platform," *ACM Computing Surveys*, vol. 52, no. 1, 2019.

[31] C. Wang, Y. Wang, Y. Chen, H. Liu, J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Elsevier Computer Networks*, vol. 170, pp. 107118, 2020.

[32] D. Kora and B. Damjanovi, "Information Security in M-learning Systems: Challenges and Threats of Using Cookies," *2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH)*, March, pp. 1–6, 2020.

[33] M. Sletten, M. Montebello, "Secure Mobile Learning," *Procedia Computer Science*, vol. 191, pp. 431–436, 2021.

[34] S. Garg and N. Baliyan, "Android security assessment: A review, taxonomy and research gap study," *Computers and Security*, *100*, 102087, 2021.

[35] S. Saikat, J. S. Dhillon, W. Fatimah, W. Ahmad, and R. A. Jamaluddin, "A Systematic Review of the Benefits and Challenges of Mobile Learning during the COVID-19 Pandemic," *education sciences*.