International Journal of Natural & Applied Science
Volume 4, Number 2, June 2023
http: / /www.cedtechjournals.org
ISSN: 2756-4606

MOBILE LEARNING SECURITY: CHALLENGES, PREVENTIVE MEASURES AND FUTURE DIRECTION

***Adamu, M., Kolo, H., Isah, A.D., and Gonna I.S.**
*Department of Computer Science, Federal Polytechnic, Bida, Niger State
[1]Department of Computer Science, Federal Polytechnic, Bida, Niger State
[2]Department of Computer Science, Niger State Polytechnic, Zungeru, Niger
[3]Department of Computer Science, Niger State Polytechnic, Zungeru, Niger
Email: bejian2004@gmail.com

ABSTRACT

There exist few literature reviews on security issues in the use of mobile devices in educational institutions, but do not sufficiently address the security challenges of the mobile learning system. Motivated by this fact, the study attempts to review security challenges in mobile learning and classified them based on the security requirement and vulnerability issue of mobile learning, highlights preventive measures and points out the current research in the area of m-learning security. To achieve the stated research goal, the study applied a systematic literature review using the PRISMA technique to put forward the quality criteria that are based on the research goal, objectives, and knowledge relevant to the study of security challenges of a mobile learning system. The paper examined studies published in 2012-2022 containing the keywords "mobile learning", "mobile education" "security challenges" and "security trends". Related articles were obtained from various databases namely Google Search, IEEE, WILEY, Scopus, ACM Digital Library, Science Direct, and Springer. In total 116related articles were initially found. Upon executing careful selection criteria, 66/39 articles were selected for final review. The results from the review reveal the scarcity of appropriate literature on security challenges in mobile learning system and that these issues are a thing of concern, and needed to be looked into in this ever-growing world of technologies. However, most of the studies reviewed lack of a comprehensive framework to demonstrate the security challenges in mobile learning. Thus, the results from this paper provide additional knowledge to the users of mobile learning as a whole; students in their usage of mobile learning, and the research community on the current security challenges in the adoption of mobile learning system.

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

INTRODUCTION

Mobile technology has taken a pivotal role in helping humanity leading to a significant medium of interaction in the social world as well as teaching and learning. The mobile learning (M-Learning) system presents to be a very needful tool for learners. It can help ease obtain study materials, knowledge, and information anytime, anywhere in their daily life. The massive use of these mobile devices like headphones, i-pads, smartphones, tablets, and PDAs is an international phenomenon. It has provided a broad encouragement in different areas like schools, colleges as well as education system (Dhara & Bandyopadhyay, 2021). Mobile learning is a learning system that involves the use of mobile devices that is made of four key aspects: input, sensing, output, and connectivity that encourage learners to learn in any place at any time outside the classroom and connect their learning experience with online information(Sophonhiranrak, 2021).Mobile learning is a growing trend as it can be exploited to the challenges of particular educational context, complement and enhances formal schooling, improve and assist learning for people across age, and income spectrums, and provide learning opportunities in communities where educational opportunities are limited (Mseteka & Phiri, 2019). The generation of mobile technologies such as Wireless networks and mobile devices has encouraged advancement in the education sector owing to the introduction of mobile learning (m-learning). Mobile learning platforms are designed to support the advances in mobile technologies to make learning ubiquitous, engaging, and flexible (Oyelere *et al.,* 2015).Mobile learning is a kind of learning method that shares and distributes information and it can be used as an alternative to the traditional classroom for learners, who may not be able to attend the traditional classroom environment (Khan *et al*., 2019). M-learning is richly supported by the convergence of internet and cyber technologies into a single entity called the internet-of-things (Oyelere *et al*., 2015). Mobile learning system uses the internet to share and distribute data and information.

However, advances in mobile technologies have placed mobile learning in the frontline of security threats. Individuals, organizations and developers pay little attentions to the security issues confronting mobile learning and security is a burning issue and often neglected (Nikhil *et al*., 2021). The internet (wireless network) as a backbone of mobile learning system is insecure and the insecurity inherited in wireless network is transferable to mobile learning system (Khan *et al*., 2019).

M-Learning systems contain a lot of very personal and business critical data which are very sensitive information and therefore needs to be protected against misuse and inappropriate access. Security aspects in m-learning environment are very important and these aspects should be addressed by ensuring that m-learning information security counter measures are implemented. Examples of business-critical data which are very sensitive information are course material, submitted assignment, results examine question and test question (Mathematics *et al*., 2018).

Amongst security issues in m-learning are protection against manipulations (i.e. from either student or insider), user authentication, and confidentiality. As m-learning functionality is expanding, information must be actively protected to avoid the loss of confidentiality, availability and integrity. Security of information is very crucial; therefore, sensitive information should be restricted only to few well defined groups. Examples of sensitive academic information are learning materials for certain groups, e-result for certain individuals and copyright protection of intellectual properties (Adetoba *et al*., 2016).

Also, vulnerability issues (limited power energy, small memory space, low computational power) in the mobile devices is transferable into m-learning system and makes it easier for attackers to disclosure, altering, and stealing of academic sensitive learning information without authorization from lecturers or owners as the use of heavy security approach cannot be enforced in mobile devices which is the principal tool used in mobile learning system (Dhanda *et al*., 2020).

The mobile devices are openly deployed and use wireless media for transmission. Open deployment makes these devices susceptible to attacks. It is quite easy to intercept a wireless transmission and alter the content of information. Given the critical nature of services, information security is of paramount importance as the interception or alteration of the information can result to loss of information (Dhanda *et al*., 2020). Mobile devices are vulnerable to security threats such as software attacks: virus, service denial, worm’s macros; hardware attacks: theft, espionage; and intellectual property attacks: copyright, piracy infringement. Due to common use, handy and portable nature of mobile devices, they tend to be prone to software, hardware attacks and cyber-attacks. The security threats in m-learning systems seems quite soaring among educators especially in developing country context such as Nigeria with enormous cybercrime, fraud, theft, copyright and internet security threat (Oyelere *et al*., 2015).

Consequently, it is important to review the existing security challenges of mobile learning in order to provide the current state of the security challenges to help mobile learning stakeholders to deploy a secure, safe and reliable mobile learning system.

The contribution of the study is of threefold. First, identifying the existing security challenges and classified them based on security requirement and vulnerability issue of mobile learning system, second, highlights preventive measures to address the security challenges to the mobile learning system, and proposing new opportunities for future research. The remaining sections of the paper are structured as follows: Section two presents related studies and reviews of mobile learning security. A comprehensive taxonomy of mobile learning security challenges screen is presented in section three. A further discussion of the classification and literature is presented in section four, followed by section five, which presents the open issues in the domain of the study, and section six, which offers research directions for future works. The conclusions are drawn in section seven.

Related Studies

Recently, a little number of studies has been carried out in the area of mobile learning security challenges or threats; these literatures do not sufficiently identify the security challenges in mobile learning system. The review papers already published in this domain are listed in Table1. In this section, the study presents reviews that have presented in the literature in order to identify those issues that have been left out and have yet to be addressed and to highlight their difference with the present study.

Table 1: Comparing the Previous Review Papers with the Present Paper

Reference	Latest Reference	Type of Article	Security threats	Limitations
Kambourakis (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	Physical threats, application-based threats, network-based threats, web-based threats, and vulnerabilities issues.	Based on user's data privacy and biometric approach may not be suitable for mobile devices
Adetoba et al. (2016)	2015	Review	Confidentiality attack, integrity attack, availability attack, authentication attack, 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
Saikat 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
Sophonhiranrak (2021)	2018	Systematic Review	Learner face network security issues when using free Wi-Fi in public place	Lacking of comprehensive discussion on security challenges as one of the most barrier factor affecting adoption of mobile learning in higher education.
Nikhil et al.	2019	Survey	Cross site scripting assaults, content assaults, cross-site	Based on survey study.

(2021)			request forgery assaults, SQL injection attack, session hijacking, DDoS attack, and Man in Middle attack.	
Criollo-c etal. (2021)	2020	Systematic Literature Review	Technological issues of mobile learning such as security and privacy	Based on the uses of mobile learning, the benefits and pending issues such education infrastructural, students' behaviours, lecturers' attitudes
Sapanca & Kanbul (2022)	2022	Survey	Confidentiality, Availability, and integrity attacks on information system	A survey study
Present review	2022	Systematic Literature Review	Confidentiality attack, integrity attack, availability attack, authentication attack, nonrepudiationattacks, 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 previous reviewed papers as shown in the table 1, the propose study reviews the exiting related literatures on security challenges to the mobile learning from 2012 -2022 to provide a more comprehensive literature works that filled the gaps and update.

Research methodology

The review provides an insight into the research gap for security challenges of mobile learning, technologies that suit the needs of learners. Following the trend in mobile learning security threats studies, considerable research on same study has been carried out, but do not sufficiently identify the security issues in the mobile learning system. The PRISMA method has been used to perform the review based on recent mobile learning security threat. The review is conducted according to using two steps, namely conducting the review including data sources, search terms, quality assessments, and inclusion and exclusion criteria and reporting the review where the result is documented.

Conducting the Review

The purpose of this study is to conduct a review related to mobile learning security challenges. The literature review is a way of obtaining a body of knowledge in the field and appraising the extent of research activities related to mobile learning security challenges.

Search Strategy

The search strategy aims to identify the most relevant and recent works carried out related to mobile learning security challenges and at the same time filter the number of publications to conduct the review. Google Scholar was estimated to be the most comprehensive academic search engine since it indexes papers from various scholarly publishers and professional societies. However, to ensure completeness of the literature review, the keyword search was also applied on some popular databases namely: Science Direct, ACM Digital-Library, IEEE XPLORE, Scopus, and Wiley. The advanced search option and a combined list of keywords are used to search related content in the database. The search formula used: (Mobile Learning) OR (M-Learning) OR (Mobile Device) OR (Security Challenges) OR (Security Threats) OR (Security Issues). In carrying out this research, different database was used as mentioned. In the six-database used, the total number of 117 articles were found, and50 articles were finally selected for the research work. Table 2 below shows the different database consulted and the total number of articles used.

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:

- Papers from 2012 to 2022.
- Articles related to learning management system.
- Articles related to benefits and challenges of mobile learning, review and survey of existing mobile learning systems.
- Articles related to security challenges of mobile learning, review and survey of existing mobile learning systems.
- Articles were peer-reviewed.
- Full article published in the English language

Exclusion criteria:

- Articles that describe systems that do not contribute original research such as security challenges of mobile learning systems.
- The mobile device must not be a laptop or Netbooks.
- The articles that do not fall in the range of 2012 to 2022

Quality assessment

A quality assessment is conducted after filtering the pre-selected studies through inclusion and exclusion criteria to meet the research quality criteria. The research was narrowed down using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) technique to put forward the quality criteria based on the research aims, objectives, and knowledge relevant to the study of mobile learning security issues (Moher et al., 2015). The following questions are used as a checklist to measure the research credibility and validity:

- Does the study contribute to the knowledge of mobile learning security issues?
- Are the findings of the study credible with valid information on mobile learning security issues?
- Are the research aims and objectives clearly articulated to bring a proper body of knowledge on mobile learning security issues?

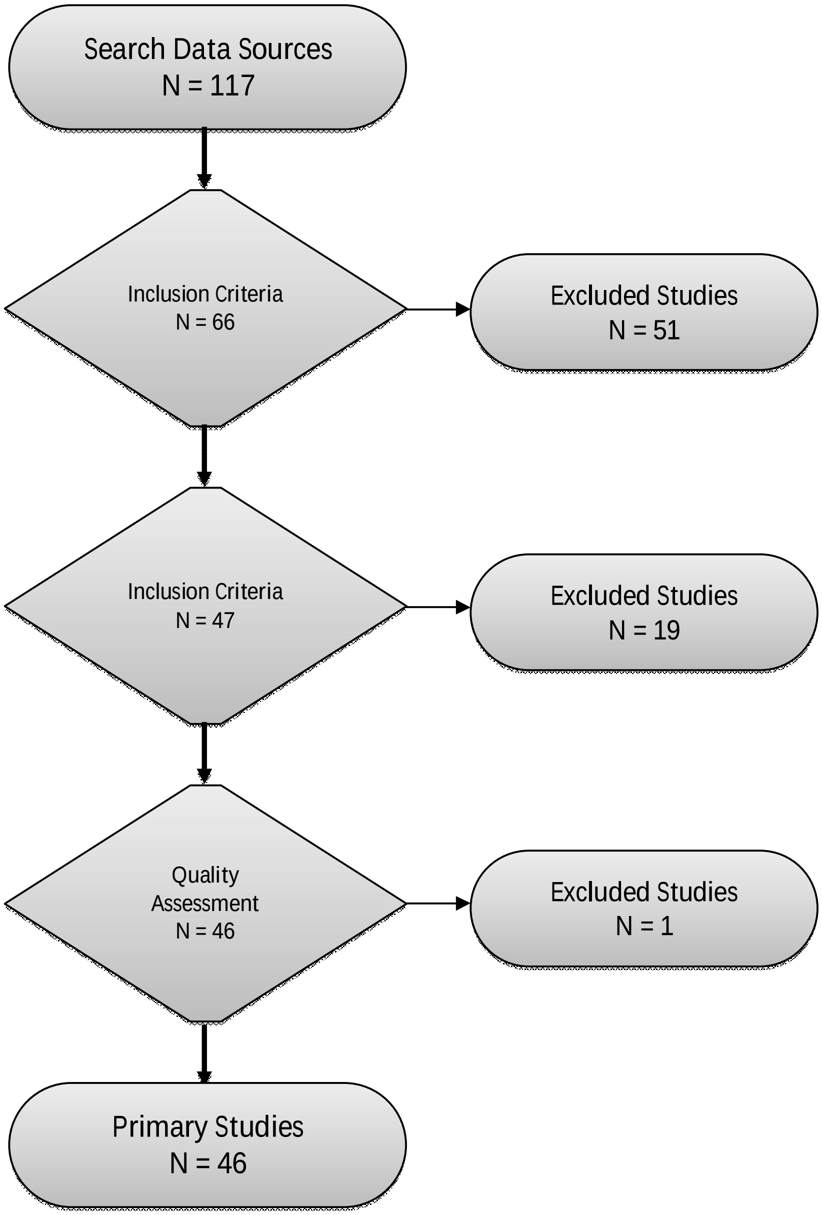

Fig. 1:PRISMA flowchart

Since all the quality assessment criteria are important in the context of the research questions, only 39 studies had been selected for the final review (Fig. 1)

Security challenges and vulnerabilities in mobile learning system

Reference	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)	√	√	√			
Qamar 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 unauthorised 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 issue:** A digital attack that penetrate mobile devices due to the weakness in the development process of mobile software or service

Preventive Measures

Based on the reviewed of related literature, it is clearly established there exist security challenges in the mobile applications and confidentiality, integrity, and availability threats are the most frequency attacks launch on the mobile applications and internet of thing applications as shown in the the security issue is still an open challenge and does not have an adequate remedy.

The following are some preventive 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 authorisation 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 note for certain individual or group, assessment records, grades, and intellectual properties should be encrypted to prevent from unauthorised 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,
- 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 asare recommended single techniques may not provide optimal solution because of limitations associated with each encryption algorithm whether 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.

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.

Future Directions

Many individuals, organisations and developers neglect security issues. As mobile learning is expanding, the security threats is growing and there is the need for individuals, organisations 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. Thus, there is 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. Also, to develop a robust hybrid dynamic lightweight cryptography model to address the security threats to ensure mobile learning system becomes secure and reliable.

REFERENCES

Abawajy, J., Huda, S., Sharmeen, S., Hassan, M. M., & Almogren, A. (2018). Identifying cyber threats to mobile-IoT applications in edge computing paradigm. *Future Generation Computer Systems, 89, 525–538*. https://doi.org/10.1016/j.future.2018.06.053

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

Al-Hunaiyyan, A., Alhajri, R. A., & Al-Sharhan, S. (2018). Perceptions and challenges of mobile learning in Kuwait. *Journal of King Saud University - Computer and Information Sciences,* 30(2), 279–289. https://doi.org/10.1016/j.jksuci.2016.12.001

Aljawarneh, S., Radhakrishna, V., & Kumar, G. R. (2019). A recent survey on challenges in security and privacy in internet of things. *ACM International Conference Proceeding Series*, 1–9. https://doi.org/10.1145/3330431.3330457

Battle, K. (2018). *Security Management for Mobile Devices of Higher Education*. Spring. Mathematics and Computer Science Capstone, La Salle University.

Bhat, P., & Dutta, K. (2019). A survey on various threats and current state of security in android platform. *ACM Computing Surveys,* 52(1). https://doi.org/10.1145/3301285

Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach : causes, challenges, prevention, and future. https://doi.org/10.1002/widm.1211

Dewan, J., & Chowdhury, M. (2013). A Framework for Mobile eLearning (mLearning) with Content Security and Authentication. *IEEE 2013 Second IIAI International Conference on Advanced Applied Informatics* 95–99. https://doi.org/10.1109/IIAI-AAI.2013.53

Diana, F., Bahry, S., Anwar, N., Amran, N., & Mohd, R. P. (2015). Conceptualizing security measures on mobile learning for Malaysian higher education institutions. 176, 1083–1088. https://doi.org/10.1016/j.sbspro.2015.01.582

Dong, X., Chen, Z., Siadati, H., Tople, S., Saxena, P., & Liang, Z. (2013). Protecting sensitive web content from client-side vulnerabilities with CRYPTONS. *Proceedings of the ACM Conference on Computer and Communications Security*, 1311–1324. https://doi.org/10.1145/2508859.2516743

Elsand W.K.(2018).Securing Sensitive Digital Data in Educational Institutions using Encryption Technology. *International Journal of Computer Science and Information Security.* Vol. 16 No 6. pp1-8. ISSN 1947-5500@IJCSIS,USA. https://sites.google.com/site/ijcsis

Garg, S., & Baliyan, N. (2021). Android security assessment: A review, taxonomy and research gap study. *Computers and Security*, 100, 102087. https://doi.org/10.1016/j.cose.2020.102087

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

Kakavand, S. (2019). The University ' s Strategy behind the Implementation of Mobile Technology in Education & User Adaptation Samaneh Kakavand To cite this version : HAL Id : tel-02048479 The University ' s Strategy behind the Implementation of Mobile Technology in Education.

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

Kambourakis, G. (2016). Security and privacy in m-learning and beyond : *Challenges and state-of-the- Security and Privacy in m-Learning and Beyond* : Challenges and State-of-the-art. January.

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

Kim, G. L., Lim, J. D., & Kim, J. N. (2017). Mobile security solution for sensitive data leakage prevention. *ACM International Conference Proceeding Series, Part F128004*, 59–64. https://doi.org/10.1145/3057109.3057117

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

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

Mathematics, A., Uniyal, A., Kumar, P., & Panwar, N. S. (2018). Enhanced USB-Token based Secure Authentication Scheme for M- Learning Applications. 119(12), 12603–12609.

Miguel, J., Caballé, S., Xhafa, F., Prieto, J., & Barolli, L. (2016). A methodological approach for trustworthiness assessment and prediction in mobile online collaborative learning. Computer Standards and Interfaces, 44, 122–136. https://doi.org/10.1016/j.csi.2015.04.008

Mohd Ishak Bin Ismail. (2016). A Review of the Challenges and Issues in Mobile Learning. *International Journal of Enhanced Research in Educational Development,* 4(2), 1–6.

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

Mseteka, L., & Phiri, J. (2019). A Secure Model for Storage and Dissemination of Examination Results : *A Case Study of Zambia Technical Education Vocational and Entrepreneurship Training Authority.* https://doi.org/10.3844/jcssp.2019.221.234

Nikhil Pinnamaneni, Sai Charan Muvva, & Sumanth Dodda. (2021). A Study on Threats to Mobile-Learning. *EPRA International Journal of Research & Development (IJRD),* 7838(July), 271–279. https://doi.org/10.36713/epra7696

Obiria, P. B., Kimwele, M. W., Cheruiyot, W. K., & Mwangi, G. (2015). A Location-Based Privacy Preserving Framework for M-Learning Adoption to Enhance Distance Education in Kenya: Literature Review. Ijarcce, 4(10), 8–13. https://doi.org/10.17148/ijarcce.2015.41002

Ochaya, W. (2018). The Cyberthreat in IoT , Mobile Learning , and Wearable Devices in Education. 1, 1–18.

Oyelere, S. S., & Malgwi, Y. M. (2015). Cybersecurity Issues on Web-Based Systems in Nigeria : M-Learning Case Study. November. https://doi.org/10.1109/CYBER-Abuja.2015.7360510

Pendhari, K., Pawar, A., Erunkar, A., Hutke, A., Sem, S. V., & Technology, I. (2017). Secure Data Storage on Cloud System for Privacy Preserving. *International Research Journal of Engineering and Technology*. Volume o4 Issue 03.pp 3–6.

Pereira, O. R. E., & Rodrigues, J. J. P. C. (2013). Survey and analysis of current mobile learning applications and technologies. *ACM Computing Surveys,* 46(2), 1–35. https://doi.org/10.1145/2543581.2543594

Sadeghzadeh, S. H., & Nakhaei, A. (2017). Proposing a Secure Architecture for Mobile-Learning Environments and Investigating Teachers' Attitude. *Interdisciplinary Journal of Virtual Learning in Medical Sciences,* 8(3), 1–8. https://doi.org/10.5812/ijvlms.64233

Saikat, S., Dhillon, J. S., Fatimah, W., Ahmad, W., & Jamaluddin, R. A. (2021). education sciences A Systematic Review of the Benefits and Challenges of Mobile Learning during the COVID-19 Pandemic.

Saxena, N., & Chaudhari, N. S. (2012). A secure approach for SMS in GSM network. ACM *International Conference Proceeding Series,* 59–64. https://doi.org/10.1145/2381716.2381729

Sapanca and Kanbul (2022) Risk Management in Digitalized Educational Environments: Teacher's Information Security Awareness Levels. doi:10.3389/fpsyg.2022.986561

Shonola, S. A., & Joy, M. (2014). Security Framework for Mobile learning environments. 7th *International Conference of Education, Research and Innovation Conference*, November, 3333–3342.

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

Shonola, S. A., & Joy, M. S. (2014). Mobile Learning Security Concerns from University Students ' Perspectives. May 2015. https://doi.org/10.1109/IMCTL.2014.7011125

Shonola, S. A., & Joy, M. S. (2015). Security of m-learning system: A collective responsibility. *International Journal of Interactive Mobile Technologies,* 9(3), 64–70. https://doi.org/10.3991/ijim.v9i3.4475

Shonola, Shaibu Adekunle, & Joy, M. (2014a). Security Framework for Mobile learning environments. *7th International Conference of Education, Research and Innovation Conference, November*, 3333–3342.

Shonola, Shaibu Adekunle, & Joy, M. S. (2014b). Investigating Attack Vectors in M-learning Systems in Nigerian Universities. 178–184.

Shonola, Shaibu Adekunle, & Joy, M. S. (2014c). Mobile Learning Security Concerns from University Students' Perspectives. May 2015. https://doi.org/10.1109/IMCTL.2014.7011125

Shonola, Shaibu Adekunle, & Joy, M. S. (2015). Investigating attack vectors in M-learning systems in Nigerian universities. *Proceedings of 2014 International Conference on Interactive Mobile Communication Technologies and Learning, IMCL 2014,* February 2015, 178–184. https://doi.org/10.1109/IMCTL.2014.7011127

Sletten, M., Montebello, M., Sletten, M., & Montebello, M. (2021). ScienceDirect ScienceDirect Secure Mobile Learning. Procedia Computer Science, 191, 431–436. https://doi.org/10.1016/j.procs.2021.07.054

Sophonhiranrak, S. (2021). Heliyon Features , barriers , and influencing factors of mobile learning in higher education : A systematic review. Heliyon, 7(October 2020), e06696. https://doi.org/10.1016/j.heliyon.2021.e06696

Study, C. (2015). Learners ' Perception on Security Issues in m-learning (Nigerian Universities Exchanges : the Warwick Research Journal Learners ' Perception on Security Issues in m-learning (Nigerian Universities Case Study) Shaibu Adekunle Shonola and Mike S Joy. February.

Tao, C., Guo, H., & Huang, Z. (2020). Identifying security issues for mobile applications based on user review summarization. *Information and Software Technology*, 122(February), 106290. https://doi.org/10.1016/j.infsof.2020.106290

Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., & Savangsuk, V. (2017). A Policy-Based Framework for Preserving Confidentiality in BYOD Environments : *A Review of Information Security Perspectives. Security and Communication Networks (WILEY).* Volume2017,Article ID 2057260, 11pages. https://doi.org/10.1155/2017/2057260.

Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. *Elsevier Computer Networks*, 170, 107118. https://doi.org/10.1016/j.comnet.2020.107118

Yuan, X., Yang, L., He, W., & Simpkins, L. (2016). Teaching security management for mobile devices. SIGITE 2016 - *Proceedings of the 17th Annual Conference on Information Technology Education*, 14–19. https://doi.org/10.1145/2978192.2978227

Yuan, X., Yang, L., He, W., & Simpkins, L. (2016). Teaching security management for mobile devices. SIGITE 2016 - *Proceedings of the 17th Annual Conference on Information Technology Education*, 14–19. https://doi.org/10.1145/2978192.2978227

Singh, M. M., Chan, C. W., & Zulkefli, Z. (2017). *Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm*.Internatioal Journal of Advanced Computer Science.*8*(2), 53–6

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