Privacy Preservation in Mobile-Based Learning Systems: Current Trends, Methodologies, Challenges, Opportunities and Future Direction

Muhammad Kudu Muhammad(✉), Ishaq Oyebisi Oyefolahan, Olayemi Mikail Olaniyi, and Ojeniyi Joseph Adebayo

Federal University of Technology, Minna, Nigeria
{muhammad_kudu,o.ishaq,mikail.olaniyi,ojeniyia}@futminna.edu.ng

Abstract. The adoption of mobile technologies in education are evolving like in the business and health sectors. The design of user-centric platform to enable individuals participate in the activities of learning and teaching is currently area of research. The Learning Management Systems (LMS) area assists learners and academic activities but, it continues to fall short of desired impact due to huge demands of the application. More importantly, the mobile applications offer enormous convenience not without the possibility of eavesdropping and maliciously exploiting data about users. The original structure of mobile learning requires that data and processing heads have centralized entity, which is not possible in wireless application arrangements due to communication overhead of transmitting raw data to central learning processor. This led to the use of distributed mobile learning structure, which preserve privacy of learners. This study discusses the challenges, current trends, methodology, opportunities and future direction of privacy preservation in mobile-based learning systems. The study highlighted the use of learners' private data and behavioral activities by LMS especially in understanding the needs of learners as well as improvement of their experiences. But, it raises concerns about the risks of learners' privacy on LMS due the mining processes of learners, which were not considered in existing related studies in literature.

Keywords: Mobile learning · Mobile-based learning system · Privacy preservation · Learning management system developers

1 Introduction

The LMS have been adopted by higher level of education (such as universities) in order to improve the practice of educators and learners, and provides learning management functionalities for these institutions [1]. One concern features prominently, which is the protection of the privacy of users. The problem of privacy continues to attract the attention of users and developers. Third parties find easy to determine actions, transaction consummated, traffic data, and location information of users for potential security and privacy compromises [2].

S. Misra and B. Muhammad-Bello (Eds.): ICTA 2020, CCIS 1350, pp. 520–534, 2021.
https://doi.org/10.1007/978-3-030-69143-1_40

The progression in vast computing and communication effectiveness of the devices and systems; there is an unprecedented ease in storing, retrieving and processing of big volumes of information [3]. In LMS, there is argument that data mining can be carried in a secure way to support private information preservation for private learning activities. Learning systems make use of data mining approaches in order to detach strong data emanating from diverse sources though certain information considered grungy is expected to be removed to protect privacy and security of individual users including identifiers, names, conveys and location information [4].

There are immersed opportunities available to several fields such as education, for harvesting and gaining valuable insight into learners' private information, which puts enormous risks on them. The Chun attributes analysis performed by operators on public database infrastructure further makes learners' data vulnerable to unrestricted invasion of privacy. The solution is to scrutinize the attributes of users' in the dataset to determine excusive and private or sensitive data requiring preservations [5]. Studies in [6–9] have confirmed the use of learners' private data and behavioural activities in LMS for the purpose of understanding the needs of learners as well as enhance their experiences. The privacy and security lapses caused by these mining processes of learners were not considered.

Therefore, this study presents a review to examine the trends of the published articles as a synthesis onto privacy preservation in mobile-based learning systems under subsections such as current trends, methodology, challenges, opportunities and future direction. This article makes the following contributions:

1. Presents the current applications and trends of mobile-based learning systems in pedagogy achievements of learners;
2. Investigate the existing problems and challenges of mobile-based learning systems inhibiting successful widespread implementation;
3. Identify the methodologies and solutions to the problems and challenges of privacy preservation of mobile-based learning system;
4. Further examine the opportunities of mobile-based learning systems;
5. Recommend on future research directions on the privacy preservation in mobile-based learning systems.

The remaining parts of the review are arranged as follows: Sect. 2 explains the previous related studies and the differences of the new study and existing studies. Section 3 presents the review methodology for the articles selection and data collection processes. Section 4 is the results presentation of data collected. Section 5 is the concluding part of the review.

2 Literature Review

The differences and similarities between the present study and the review of selected studies or articles, which serve as the justifications of this study is presented in Table 1.

Table 1. The differences between the existing related studies selected and this study.

Author(s)	Domain of study	Type of article	Privacy and security considerations
[6]	Adaptive e-learning system	Systematic Literature Review	Only offers personalised and self-directed learning environment without considerations for privacy and security
[7]	Learning Management System	Review	Highlights use of LMS for teaching and learning in institutions. Provide less considerations for privacy
[13]	E-Learning Systems	Systematic Literature Review	Individual and social sustainability meta-requirements of e-learning systems
[11]	Learning Management System	Review	-Blurred data elements for privacy of learners was reported and behavioural patterns of learners are a key to LMS
[15]	Learning Management System	Review	Provides the information necessary to develop highly adaptive and person-centred LMS and uses unified theory of acceptance and use of technology (UTAUT) to mine learners' data, without considerations for privacy and security
[12]	Smart Big Data Analytics in Healthcare	Systematic Literature Review	The video-based continuous tracking of human activities through cameras deployed in rooms raises privacy issues
[14]	Learning Management System	Full-article	Only highlights behaviour of teachers to LMS in universities, trust and UTAUT 2 approaches were used to identify factors impacting acceptance without considerations for privacy and security
[8]	Learning Management System	Review	Explores learners' interactions and behaviours patterns with LMS and focuses on learning analytics and educational data mining as key part of LMS without considerations for privacy and security
[10]	Knowledge Sharing	Systematic Literature Review	Explain social media sites without considerations for privacy and security

From Table 1, there are opening for further investigations on ways of evolving novel learning analytics approaches grounded on secure learning process mining for better learning situations through the use of learners' data [8]. There is no definite consideration on the concerns posed by security and privacy issues about platforms, and tools applicable for knowledge sharing [10]. There are quite a number of confirmations on the use of learners' private data and behavioral activities by LMS especially in studying and understanding the needs of learners as well as improvement of their experiences. The data assists in situating technology for educational purposes; it increases in the risks of learners' information on LMS. Specifically, the privacy and security lapses caused by these mining processes of learners were not considered by [6–9]. There is general consensus on the fact that learners' behavioral patterns and personal data are often harvested by many LMS deployed for teaching and learning in educational setups. This learner information mining is a veritable process for the proper functioning of LMS. This study focuses on the issues arising from legitimate use of learners' data for providing better learning experiences using selected studies in the next section.

2.1 Related Studies

In recent time, many studies were conducted to review and survey the conventional learning management system (LMS) domain. Amongst earlier significant works of [9] who introduced a review on the mobile-based learning systems. The authors analyzed and explore learners' interactions and behaviors patterns with LMS advantages and limitations related to learning analytics and educational data mining as key part of LMS. However, the review do not consider the issues of privacy and security.

Many other SLR studies in privacy preservation in mobile-based learning systems were also presented. For instance, [10] in knowledge sharing domain conducted a SLR and ascertain there is lack of focus on the impact of security and privacy concerns about platforms, and tools applicable for knowledge sharing through social media sites. A related work in [11] reported on there are review that there is blurred data elements for privacy of learners and behavioral patterns of learners are a key to LMS. With remarkable SLR of [12] in Smart Big Data Analytics in Healthcare with video-based tool continuous tracking of human activities through cameras deployed in rooms detecting privacy issues.

However, [12] is on health application area which also be applied in educational area particularly in distance learning environment. Also, the SLR of [6, 13] both in e-learning domain described the personalized learning environment, self-directed, individual and social sustainability meta-requirements of e-learning systems as its related to privacy. Recently, [14] highlights behavior of teachers to LMS in universities. Trust and UTAUT 2 approaches were used to identify factors impacting acceptance (privacy preservation metrics). [7, 15] both reviewed they are articles in LMS domain with similarities in their strengths and weaknesses. According to the [7] the use of LMS for teaching and learning in institutions globally is the strength while missing of virtual laboratory from the review of the LMS is a limitation.

The later [15] provides the information necessary to develop highly adaptive and person-centered LMS and uses unified theory of acceptance and use of technology (UTAUT) to mine learners' data. Similarly, [9] SLR in Digital Technology based learning and education domain identifies ways of deepening technology in educational sector

and improve students-teacher experiences. Hence, the review uses search strategy and selection criteria following the guidelines used by Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) technique. Next section explained the justification for this study.

2.2 Mapping of the Study

The mapping justifies the highest influence and association to the present study as realized from the connected papers' prior and derivative studies graph built illustrated in Fig. 1.

Fig. 1. Privacy-preserving learning analytics: challenges and techniques.

In Fig. 1, this study included studies outside of the scope of the mapping article especially including post-2020 era. This present review paper is a derivative work encompassing fresh subjects related to privacy of mobile learning systems and Big Data applications. It serves as the reason for embarking on this study in order to cover for the gaps in the existing studies.

3 Review Methodology

This study discusses the research questions and the methodology for conducting the Systematic Literature Review (SLR) using the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) technique.

3.1 Research Questions

This survey makes use of the following research questions:

1. What are the current applications and trends of mobile-based learning systems in pedagogy achievements of learners?
2. Are there existing problems and challenges of mobile-based learning systems inhibiting successful widespread implementation?
3. What are the best methodologies and solutions to the problems and challenges of privacy preservation of mobile-based learning system?
4. Are there opportunities of mobile-based learning systems?
5. What are the future research directions on the privacy preservation in mobile-based learning systems?

The purpose of the review is to systematically develop the concise stages for the proposed research. This method of study involves Planning and specifying research questions, conducting the review (that is, an identification of search string and data sources, selecting studies, quality assessment, and data extraction and finally reporting the review [16]. In order to achieve this, the preferred reporting items as reported by [13, 16]. The inclusion and exclusion criteria include all published peer reviewed articles from five major criteria established for this study as shown in Fig. 2. The criteria for data extraction or inclusion in this study include:

1. Articles details the first author, country and type of paper.
2. Articles in the categories of technical reports, journals, conference proceedings and reviews/surveys.
3. Articles published with the timeline of January 2013 to January 2020.
4. Articles related to the keywords or concepts of this study such as Mobile Learning, Privacy and Security, Big Data Mining Procedure, and Data Management for Learners.
5. Articles written in the English Language.

The manual and autonomous search for this study involves a series of search strings across the titles, the abstract, and keywords fields of the articles in digital libraries as follows: (privacy and security in mobile learning systems) AND (data mining techniques in learning management systems) AND (challenges and issues of mobile learning management systems) AND (electronic or learning management systems) AND (privacy and security solutions to learners' data mining). The records sources for the study include: ResearchGate, Springer Link, ACM Digital Library, Scopus, Wiley, Thompson Reuters, IEEExplore Digital Library, Google Scholar, and Elsevier.

From Table 2, the research area enjoys biggest activities in the years covering 2018 and 2019 with 38.71% and 19.35% respectively. The trend revealed popularity of the technology in pedagogy in teaching and learning especially in the year 2018 but decreased considerable afterwards due to several challenges of security and privacy of learner's data mining for legitimate and unapproved usages in year 2019 according this new study.

The timeline for the study and quantity of records returned in terms of percentages matching the year are presented in Table 2.

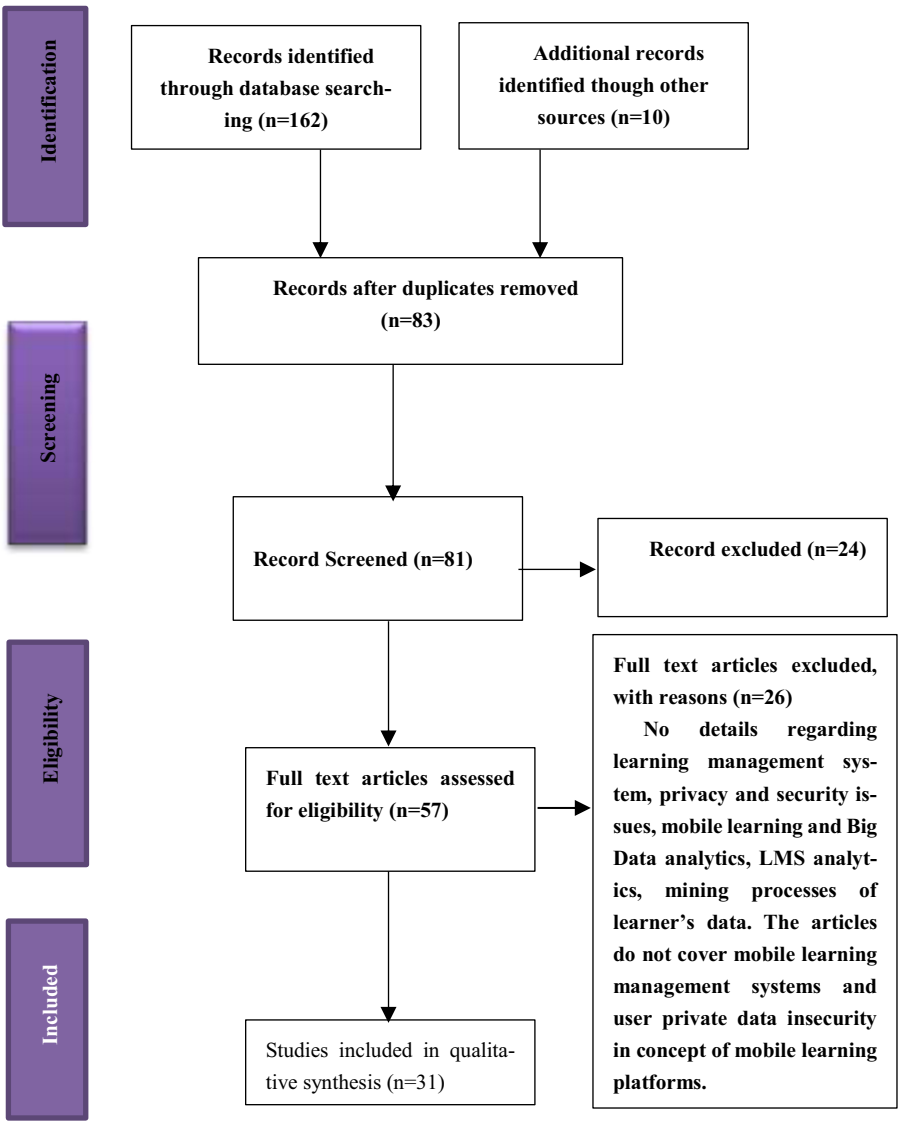

Fig. 2. The review workflow with PRISMA.

Table 2. Timeline of published articles.

Year of publication	Quantity returned	Percentage (%)
2020	1	3.23
2019	6	19.35
2018	12	38.71
2017	5	16.13
2016	5	16.13
2015	0	0.00
2014	1	3.23
2013	1	3.23
Total	31	100

4 Results and Discussion

The answers to the research questions (that is, research questions 1–5) are presented in the next subsections as follows:

4.1 Current Trends

The current trends of this study explain the period of research activities from year 2013 to 2020 as depicted in Fig. 3.

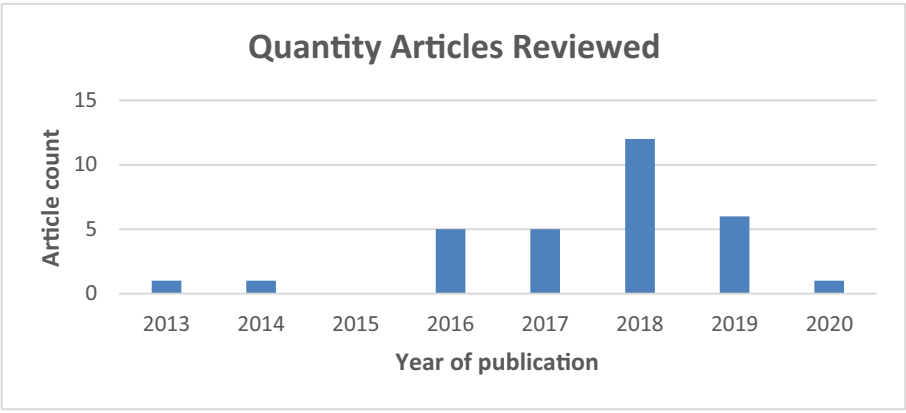

Fig. 3. Current trends of review from 2013–2020.

From Fig. 3, the research activities were most pronounced in the year 2018, but reduced significantly in the year 2019. These changes can be explained as general acceptance of technology for the business of teaching and learning in higher institutions but,

the privacy and security issues of learner's data during analytics exposed more risks of learning management systems supported by mobile and handheld devices on the basis of this new study.

4.2 Challenges and Issues of Mobile-Based Learning System and Its Applications

This study identified issues related to mobile-based learning system and its applications domain as presented in Table 3.

Table 3. The challenges and issues of mobile-based learning system.

Author(s)	Domain	Application area	Issues identified
[1, 5, 17–21, 26–34]	Big Data	E-Security, E-Health, E-Leaning systems, data analytics, online merchandize, cyberspace, Human Computer Interaction	Privacy, security, large dataset, identity/attributes disclosure, storage, authentication, usability, unauthorized access, data sharing, technology integration, verification, data collection, poor framework, large communication overheads, and third-party services
[23–25]	Educational	Mobile learning, learning analytics, online learning	Privacy, threats to physical learning devices, data in cloud protection, sensitive data disclosure, data tracking, evaluation of learners, access to resources and services, latency, outliers and information generation
[22]	Cloud computing	Mobile cloud computing	Location privacy, identity privacy, mobile device security, security, partitioning and offloading security, visualisation, data loss and recovery

From Table 3, the general setups for m-learning needs safeguards mechanisms to preserve private and sensitive data concerning actors (or learners) [1, 23–25, 28, 31]. A number of these private sensitive data of learners have been identified including

[24]: name, gender, birth data, address, credit card details, biometric characteristics of actors, mobile phone number, email address, location data, IP address, IMEI, location data, service usage data, e-mail, call record and web-browsing log files and history, and security credentials. According to the study in [18], the birth of Big data has given rise to several issues of security and privacy due to the need to perform analytics and mining of private and sensitive data of users' datasets for diverse applications such as medicals, educational, etc. There are the general concerns about users losing their privacy rights regardless of the fact that the enormous datasets have potential benefits to the society and improving application effectiveness. In addition, several quantities of data concerning users are available on Big Data applications including: Internet activity, demographic information, content usages, private data, which are harvested and analyzed by several organizations for surveys. These activities are highly harmful to the users and data providers because sensitive data and identity of users can be divulged [17]. Individuals become sensitive to the need for privacy of their health information in cases of terminal and serious illness disclosure [29].

4.3 Existing Methodology and Solutions to Privacy and Security

There are several of methodologies and solutions to privacy and security of Big Data and its applications (that is, mobile-based LMS) in different domains along with weaknesses are presented in Table 4.

Table 4. The methodologies and solutions to privacy and security of Big Data.

Author(s)	Domain	Methodology/solution	Weakness
[1, 5, 17, 18, 26–34]	Big Data	- Encryption, cryptosystems and intrusion detection systems - Personalised services	- Re-identification - Private data access - Convergence
[23–25]	Educational	- Data mining, visual data analysis techniques	- Privacy, ethical and risks to learners' data
[21, 22]	Cyberspace	- Infrastructure security layers, cryptography, data provenance, secure and distributed computing, access controls	- Vulnerable to attacks during data usages
[22]	Cloud computing	- Data partitioning strategy (sensitive and non-sensitive), secure socket layer, encryption and cryptography, strong authentication and access control schemes	- Computational and performance degradation - Cloud and mobile device integration complexities

From Table 4, the privacy of data during storage, access and manipulations pose major challenges which is gaining interests. There are no privacy guarantees for private data elements in users' dataset during the process of content mining for diverse applications. A number of anonymization techniques make use of machine learning analysis to isolate and mask personal identifiers in datasets to enforce privacy of users. Cryptographic, encryption, data partitioning strategy, intrusion detection systems are often used to mitigate privacy and security issues in Big Data and its applications.

4.4 Opportunities and Future Directions

The popularity and dominance of Big Data, have opened the opportunities for improving teaching and learning activities, and the learning situations in LMS and mobile-based LMS as presented in Table 5.

Table 5. The opportunities of mobile-based LMS.

S/N	Author (s)	Opportunities for mobile-based LMS
1	[7, 8, 11, 14]	Data acquisition
2	[7, 8, 11]	Storage
3	[6–8, 11, 14, 35]	Data analysis
4	[6–8, 11, 35]	Data visualization
5	[6–9, 11, 14, 15, 35]	Learning process
6	[6–9, 14, 35]	Learning achievements

This study found from literatures that, many researchers and scholars have identified the needs to increase security requirements of Big Data and mobile-based LMS to support data analysis, transfer, acquisition and storage while overcoming data leakages [18, 28]. There are needs to ascertain the effectiveness of common privacy preservations schemes identified by this study for Big data and its applications (or micro-data) including cryptography, perturbation, anonymization, randomized response and condensation [5, 17, 29]. The future data privacy schemes must investigate inherent capabilities of machine learning algorithms in protecting mobile-based LMS private user data [18, 32]. More so, the masking techniques should not only add noise and decrease quality, but dimensionality decrement too to fit into prevailing bandwidth and storage requirements of mobile-based LMS [30, 33].

4.5 Future Directions

The concerning issues relating to LMS its applications, and suggestions for further probing are highlighted on the bases of selected studies and articles in Table 6.

From Table 6, researchers and scholars have identified the needs to focus attention on authentication and authorization schemes for Educational and its applications (such as

Table 6. The issues of Big Data and its applications for future directions.

S/N	Author	Domain	Solution proposed of future investigations
1	[1, 5, 17–21, 26–33]	Big Data	- Monitoring of network traffic to detect suspicious behaviours fast - Transferable data must be encrypted with proper standard in accordance: data type - Users and devices need to be granted access to be able to use resources - All communications should take place over secure channels - Personal data should be masked prior to the publish of the dataset
2	[23, 24, 25,]	Educational	- Data privacy is a problematic. Despite progress in s technical solutions, there are still complexities in defining privacy and inherent limitations of privacy-preserving mechanisms
3	[22]	Cloud Computing	- There is need to reduce overheads during communication and computation for improved mobile devices effectiveness

mobile-based LMS) because of their capabilities to protect privacy of application users and other private dataset through anonymizations and encryption methods. In fact, there is need to increase security requirements of Big Data and mobile-based LMS to support data analysis, transfer, acquisition and storage while overcoming data leakages [18].

The anonymization schemes have recognised as effective in providing k-anonymity and its operators in order to protect micro-data. The main idea is to make user private data elements or attributes indistinguishable, which can be applied in education and medicine [17]. There is need to investigate machine learning pre-processing approach such as dimensionality minimisation and sampling which can be integrated in to appropriate data masking techniques for preserving privacy. More so, the masking techniques should not only add noise and decrease quality, but dimensionality decrement too to fit into prevailing bandwidth and storage requirements of mobile-based LMS [30].

5 Conclusion

This study found that a number of terminologies have been given to the process of deploying technology to share knowledge including mobile learning, digital learning, and electronic learning. The learning management system make use of pedagogical infrastructures, human interaction, learning content and evaluation support to enhance teaching and learning events in higher institutions of learning.

There is quest at present to meet the needs of learners when it comes to the learning process and content distributions. The Learning Management System and its applications have become commonplace procedures for storing, analyzing, integrating and visualizing

of large data of users in easier ways. One of the main applications of Big Data in education is the mobile-based LMS that support distrusted and learner-centered learning process.

There are efforts to protect learner's data from unauthorized and inordinate exposure of privacy which have raised security concerns about mobile based learning management systems [5]. The future works are to consider the best ways of performing mining operations on learner's data without fear of privacy compromises. Also, there is need to determine the private elements of learner's data using machine learning algorithms alongside appropriate privacy preservation approaches.

References

1. Singh, H., Miah, S.J.: Design of a mobile-based learning management system for incorporating employment demands: case context of an Australian University. Educ. Inf. Technol. **24**(2), 995–1014 (2018). https://doi.org/10.1007/s10639-018-9816-1
2. Wang, Y., Zheng, N., Xu, M., Qiao, T., Zhang, Q., Yan, F.: Hierarchical identifier: application to user privacy eavesdropping on mobile payment app. Sensors **19**(14), 1–9 (2019). https://doi.org/10.3390/s19143052
3. Ketthari, M.T., Rajendran, S.: Privacy preserving data mining using hiding maximum utility item first algorithm by means of grey wolf optimisation algorithm. Int. J. Bus. Intell. Data Min. **14**(3), 401–418 (2019)
4. Mohanrao, M., Karthik, S.: Privacy preserving for global data using ensemble approach. In: International Conference on Computer Vision and Machine Learning, vol. 1228, pp. 1–7 (2019). https://doi.org/10.1088/1742-6596/1228/1/012046
5. Nagaraj, K., Sharvani, G.S., Sridhar, A.: Encrypting and preserving sensitive attributes in customer churn data using novel dragonfly based pseudonymizer approach. Information **10**(9), 1–21 (2019)
6. Normadhi, N.B.A., Shuib, L., Nasir, H.N., Bimba, A., Idris, N., Balakrishnan, V.: Identification of personal traits in adaptive learning environment: systematic literature review. Comput. Educ. **130**, 168–190 (2019). https://doi.org/10.1016/j.compedu.2018.11.005
7. Aldiab, A., Chowdhury, H., Kootsookos, A., Alam, F., Allhibi, H.: Utilization of learning management systems (LMSs) in higher utilization of learning management systems in higher education system: a case review for Saudi Arabia. Energy Procedia **160**, 731–737 (2019). https://doi.org/10.1016/j.egypro.2019.02.186
8. Juhanak, L., Zounek, J., Rohlíkov, L.: Using process mining to analyze students' quiz-taking behavior patterns in a learning management system. Comput. Hum. Behav. J. **92**, 496–506 (2017). https://doi.org/10.1016/j.chb.2017.12.015
9. Sarker, N.I., Wu, M., Cao, Q., Alam, G.M.M., Li, D.: Leveraging digital technology for better learning and education: a systematic literature review. Int. J. Inf. Educ. Technol. **9**(7), 453–461 (2019). https://doi.org/10.18178/ijiet.2019.9.7.1246
10. Ahmed, Y.A., Ahmad, M.N., Ahmad, N., Zakaria, N.H.: Social media for knowledge-sharing: a systematic literature review. Telematics Inform. **37**, 72–112 (2018). https://doi.org/10.1016/j.tele.2018.01.015
11. Cantabella, M., et al.: Analysis of student behavior in learning management systems through a big data framework. Future Gener. Comput. Syst. **90**, 262–272 (2019). https://doi.org/10.1016/j.future.2018.08.003
12. Ismail, A., Shehab, A., El-Henawy, I.M.: Healthcare analysis in smart big data analytics: reviews, challenges and recommendations. In: Hassanien, A.E., Elhoseny, M., Ahmed, S.H., Singh, A.K. (eds.) Security in Smart Cities: Models, Applications, and Challenges. LNITI, pp. 27–45. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-01560-2_2

13. Alharthi, A.D., Spichkova, M., Hamilton, M.: Sustainability requirements for eLearning systems: a systematic literature review and analysis. Requirements Eng. **24**(4), 523–543 (2018). https://doi.org/10.1007/s00766-018-0299-9
14. Antonius, H., Widjaja, E., Santoso, S.W., Petrus, S., Cahyadi, J.: The enhancement of learning management system in teaching learning process with the UTAUT2 and trust model. In: 2019 International Conference on Information Management and Technology, vol. 1, pp. 309–313. IEEE (2019)
15. Garone, A., et al.: Clustering university teaching staff through UTAUT: implications for the acceptance of a new learning management system. Br. J. Educ. Technol. **50**(5), 2466–2483 (2019). https://doi.org/10.1111/bjet.12867
16. Kaur, A., Kaur, K.: Systematic literature review of mobile application development and testing effort estimation. J. King Saud Univ.-Comput. Inf. Sci. (2018). https://doi.org/10.1016/j.jksuci.2018.11.002
17. Karle, T., Vora, D.: PRIVACY preservation in big data using anonymization techniques. In: 2017 International Conference on Data Management, Analytics and Innovation, pp. 340–343 (2017). https://doi.org/https://doi.org/10.1109/ICDMAI.2017.8073538
18. Bashari, B., Akbarzadeh, N., Ataei, P., Khakbiz, Y.: Security and privacy challenges in big data era. Int. J. Control Theory Appl. **9**(43), 437–448 (2016)
19. Fatt, Q.K., Ramadas, A.: The usefulness and challenges of big data in healthcare. J. Healthc. Commun. **3**(2), 1–4 (2018). https://doi.org/10.4172/2472-1654.100131
20. Simo, H.: Big data: opportunities and privacy challenges, pp. 1–21 (2018)
21. Kaushik, M., Jain, A.: Challenges to big data security and privacy. Int. J. Comput. Sci. Inf. Technol. **5**(3), 3042–3043 (2014)
22. Baqer, M., Azad, A.K., Vasilakos, A.: Security and privacy challenges in mobile cloud computing: survey and way ahead. J. Netw. Comput. Appl. **84**, 38–54 (2017). https://doi.org/10.1016/j.jnca.2017.02.001
23. Avella, J.T., Kebritchi, M., Nunn, S.G., Kanai, T.: Learning analytics methods, benefits, and challenges in higher education: a systematic literature review. Online Learn. **20**(2), 13–29 (2016)
24. Kambourakis, G.: Security and privacy in m-learning and beyond: challenges and state-of-the-art. Int. J. U- and E-Serv. Sci. Technol. **6**(3), 67–84 (2013)
25. Gursoy, M.E., Inan, A., Nergiz, M.E., Saygin, Y.: Privacy-preserving learning analytics: challenges and techniques. IEEE Trans. Learn. Technol. **114**, 1–4 (2018)
26. Manogaran, G., Thota, C., Lopez, D.: HCI Challenges and Privacy Preservation in Big Data Security. The Advances in Human and Social Aspects of Technology (AHSAT) Book Series, pp. 1–23 (2018). https://doi.org/https://doi.org/10.4018/978-1-5225-2863-0.ch001
27. Kabassi, K., Alepis, E.: Learning analytics in distance and mobile learning for designing personalised software. In: Virvou, M., Alepis, E., Tsihrintzis, G.A., Jain, L.C. (eds.) Machine Learning Paradigms. ISRL, vol. 158, pp. 185–203. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-13743-4_10
28. Niknam, S., Dhillon, H.S., Reed, J.H.: Federated learning for wireless communications: motivation, opportunities and challenges, pp. 1–6 (2019). arXiv:1908.06847v3
29. Esmaeilzadeh, P.: The effects of public concern for information privacy on the adoption of health information exchanges (HIEs) by healthcare entities. Health Commun. **34**, 1202–1211 (2018). https://doi.org/10.1080/10410236.2018.1471336
30. Torra, V., Navarro-Arribas, G.: Big data privacy and anonymization. In: Lehmann, A., Whitehouse, D., Fischer-Hübner, S., Fritsch, L., Raab, C. (eds.) Privacy and Identity Management, vol. 498, pp. 15–26. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-55783-0_2
31. Merceron, A.: Educational data mining/learning analytics: methods, tasks and current trends. In: 2015 Proceedings of DeLFI Workshops, pp. 101–109 (2015)

32. Wang, Y., Tian, Z., Zhang, H., Su, S., Shi, W.: A privacy preserving scheme for nearest neighbor query. Sensor **18**(8), 1–4 (2018). https://doi.org/10.3390/s18082440
33. Hadioui, A., Faddouli, N.E., Touimi, Y.B., Bennani, S.: Machine learning based on big data extraction of massive educational knowledge. IJET **12**(11), 151–167 (2017)
34. Plamondon, R., Pirlo, G., Anquetil, É., Rémi, C., Teulings, H.-L., Nakagawa, M.: Personal digital bodyguards for e-security, e-learning and e-health: a prospective survey. Pattern Recogn. **81**, 633–659 (2018). https://doi.org/10.1016/j.patcog.2018.04.012
35. Omolade, A.O.: Predictors of use of mobile applications by university students in Oyo State, Nigeria. J. Inf. Sci. Syst. Technol. **1**(1), 34–48 (2017)