LEARNERS' DATA PRIVACY PRESERVING SCHEME (LDPPS) IN MOBILE LEARNING SYSTEM: A PERMISSIONED BLOCKCHAIN SOLUTION

MUHAMMAD KUDU MUHAMMAD, ISHAQ OYEBISI OYEFOLAHAN, OLAYEMI MIKAIL OLANIYI, OJENIYI JOSEPH ADEBAYO, LOSOTTE YAKUBU BOYI-MUSA AND OLUWASAYO EKUNDAYO

Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria
Africa Centre of Excellence on Technology Enhanced Learning, National Open University of Nigeria, Abuja, Nigeria
Department of Cyber Security, National Open University of Nigeria, Abuja, Nigeria
Department of Cyber Security, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria
Department of Computer Science, Kwara State University, Malete, Nigeria
Email: Muhammad_kudu@futminna.edu.ng **Phone No:** +2348030594142

Abstract

The use of learning technology has significantly improved the face-to-face learning environments and the general adoption of the open and distance learning (ODL), which augmented the classical learning systems. ODL Data Lake serves as primary digital repositories for materials and resources for several individuals for the purpose of teaching and learning activities among staff, learners' and institutions. There are cases of insecurity arising from learners' interaction with learning resources from different locations. These are often possible because of vulnerable, weak authentication schemes and the difficulty confirming learners' identity. This further echoed the need for adequate security tool in m-learning environments to forestall present and future issues. Therefore, the article attempted to develop an appropriate access and authorisation scheme based on blockchain technology for preserving privacy of learners' sensitive data) enrolled in MLS. On the Permissioned Blockchain solution, Learners' Data Privacy Preserving Scheme runtime (or processing time), the proposed hashing scheme (4.95%) was higher than SHA-1 (2.30%), SHA-224 (2.23%), SHA-256 (4.28%), SHA-384 (3.51%), and SHA-512 (2.67%) for processing time. Conversely, the proposed hashing scheme trailed behind high-performing hashing schemes: BCrypt (45.56%), and PBE (34.50%), which revealed that, higher runtime values offered better privacy of information on the blockchain technology and its functions. The contributions / findings of the study were that approach helps maintain scalability while preserving data privacy. Decentralised nature ensures that no single entity has control over the learners' data, enhancing privacy and feature crucial for preserving the integrity of learners' data and preventing unauthorized modifications. Finally, create a secure and privacy-preserving environment for learners' data, ensuring that it remains confidential, tamper-proof, and accessible only to authorised parties.

Keywords: Privacy Preserving, Security, Cryptography, education and Data model

Introduction

Majority of present-day learning pedagogy utilise the relationships between multimedia, individuals, places, physical objects and events. Mobile learning systems are basically providers of learners' data, learning stimuli, learning resources, experiences of learners, location of learners, and cloud services. There is strong interdependence between the actors namely LMS sources, learning devices and cloud infrastructure which enable learners and learning platforms susceptible to security and privacy risks (Caviglione & Coccoli, 2020). The opportunity to utilise learning technologies brought about learning operations in which personal sensitive attributes such as Matric/registration number, date of birth, contact address, CGPA and Medical records about learners and learning environments are collected.

Afterward, they are analysed, measured and reported in online distance learning of exposing and interfering into individuals' private or sensitive attributes in the cloud big data to the effect of causing harm on sub-consciousness, profiling, stalking and theft (Muhammad, 2024; Atasoy *et al.,* 2020).

Mobile devices (tablets and phones) are relatively most common digital technology on earth when contrasted to downward trends in desktop and laptop computer owners. These devices are capable of harvesting trace data, which are digital records of learners whenever they make use of the learning technology and platforms (Bernacki *et al.,* 2019). The introduction of m-learning by educational institutions encouraged the use of mobile technologies to disseminate learning services is considered as a new normal (or inevitable). Though, the various digital and innovative technologies implementation are faced with certain critical challenges (Caviglione & Coccoli, 2020).

Data privacy protects information from unauthorised and a malicious access that discloses, modifies, attacks, or destroys the data stored or shared online (Ali *et al.,* 2018). According to (Muhammad *et al.,* 2023), learners' personal data security continues to hamper the full fledge adoption of mobile learning technologies. In particular, local privacy of learners is susceptible to compromises while sensitive data is processed or stored in m-learning systems. And, the use of cryptographic techniques – sensitive attribute fields are anonymised to remove links to learners' location and personal data by introducing noise and randomness to achieve the privacy preserving (Goswami, 2017).

Permissioned Blockchain deployments for privacy preserving have many benefits that reduces shortfalls cause by digital disruptions, which can be lead to breaches of private information and security. The benefit of cryptography scheme to provide protection to data integrity, authorisation and private information (Privacy preservation) stated by (Aly *et al.,* 2019). According to (Hassan *et al.,* 2019), indicated that Blockchain technology solutions are capable in resolving privacy issues of learner(s) profiles in mobile-based management system. In this Permissioned Blockchain technology particularly hashing method is used. The later approach is further investigated by "Permissioned based Blockchain Privacy preserving Scheme" developed. This article deals with the collection and handling of both learner's location and personal data.

This article is organized as follows: Section II summarises the related works, Section III also summarises the methodology. Section IV contains results and discussion. Concluding and suggestion for future work is in Section IV.

Statement of the Problem

Permissioned Blockchain Based Solution Scheme solved the challenges confronting learners' sensitive data privacy in Mobile Learning System environment. Therefore, a permissioned blockchain based automated access-control manager that authorised, authenticate and verified the require trust in a third part being envisaged in recent times for privacy information system issues, including mobile device and personal data in mobile learning system. The study focuses on the issues arising from genuine use of learners' data being location or personal for providing better learning experiences without compromising privacy.

Related Studies

The general setups for m-learning needs serious safeguards mechanisms to preserve private and sensitive data concerning actors (or learners) (Revathi *et al.,* 2021; Marjit and Kumar, 2020; Ketthari and Rajendran, 2019; Mohanrao and Karthik, 2019; Nagaraj *et al.,* 2019; Normadhi *et al.,* 2018; Aldiab *et al.,* 2019; Juhanak *et al.,* 2017; Sarker *et al.,* 2019; Avella *et*

al., 2016; Singh and Miah, 2019; Niknam *et al.,* 2019). A number of these private sensitive data of learners have been identified including: (Revathi *et al.,* 2021; Marjit and Kumar, 2020; Ketthari and Rajendran, 2019; Mohanrao and Karthik, 2019), Matric/Registration Number, gender, Date of birth, Contact address, credit card details, biometric characteristics of a actors, Mobile number, email address, IP address, IMEI, Geolocation based data, service usage data, e-mail, call record, Web browser, Browsing history, and security credentials. According to the study in Bashari *et al.,* (2016), the birth of Big data have given rise to several issues of security and privacy due to the need to perform analytics and mining of private and sensitive datasets of users for diverse applications such as medicals, and educational. These activities are highly harmful to the user and data providers because sensitive data and identity of users can be divulged for surveys. Individuals become sensitive to the need for privacy of their health information in cases of terminal and serious illness disclosure (Esmaeilzadeh, 2018). The rate of awareness of privacy and security in previous studies are summarised in Table 1.

Table 1: Related articles to m-learning as: Taxonomy (Muhammad, 2024)

S/N	Author(s)	Domain of study	Privacy and security considerations
1.	Cantabella *et al.,* 2018	Mobile Learning Systems	-Privacy of learners' data elements. -Learner behavioural patterns.
2.	Niknam *et al.,* 2019	Mobile Learning Systems	-Private data of actors or learners needs privacy protection.
3.	Revathi *et al.,* 2021	Mobile Learning Systems	-Safeguards for learners' private information.
4.	Atasoy *et al.,* 2020	Mobile Learning Systems	-Learner information and learning analytics breach privacy. -Possibility of stalking, theft and sub-consciousness.
5.	Hima *et al.,* 2021	Mobile Learning Systems	-Learning performance and feedback tools are privacy-prone.
6.	Prinsloo *et al.,* 2021	Mobile Learning Systems	-Feedback tool in LMS provides learner activities and personal information. -Security, ethics, and privacy issues are increasing.
7.	Djeki *et al.,* 2022	Mobile Learning Systems	-Security and privacy of data.
8.	Badlani *et al.,* 2022	Educational	-Learner and learning content protection. -Security and privacy of data
9.	Sanjakar *et al.,* 2022	Educational	-Security and privacy of learning contents
10.	Sivadanam *et al.,* 2022	Adaptive learning system	-Integrity -Privacy and security of data
11.	Jian-Foo Lail, Swee-Heng, 2022	Mobile Learning Systems	-Security and privacy of data
12.	Karthikegan Nagarai, 2023	Educational	-Confidentiality -Privacy and security of data

From Table 1, are still opened for further investigations by evolving novel mobile learning privacy approaches grounded on secure learning process mining for better learning situations through the use of learners' data (Juhanak *et al.,* 2017). There is no definite consideration on the concerns posed by security and privacy issues about platforms, and tools applicable for knowledge sharing (Ahmed *et al.,* 2018). There are considerations and focuses on the issues arising from legitimate use of learners' data and mobile devices for providing better learning experiences. In general, researchers and scholars have identified the needs to focus attention on authentication and authorisation schemes for distance learning and its applications (such as m-learning) because of their capabilities to protect privacy of learners' data and other private dataset through anonymisations and encryption methods. The main idea is to make user private data elements or attributes indistinguishable, which can be applied in education and medicine on storage requirements of ODL centres (Muhammad, 2024). Specifically, the privacy and security lapses caused by mining processes of learners were not considered by (Cao & Zhu, 2021; Djeki *et al.,* 2022).

The term blockchain is coined from block and chain, as a ledger system composed of a chain of blocks (Grima *et al.,* 2021; Sivadanam *et al.,* 2022). The data and hash can be defined as follow (Vatsaraj *et al.,* 2021): Hash algorithms take the variable length input string and give out a fixed length output such as SHA-256 hashing algorithm. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency [40]. Users transact with their private key and public key without any real identity exposure (Badlani *et al.,* 2022; Salman *et al.,* 2019; Sanjekar and Patil, 2022; Shrivastava *et al.,* 2019; Mohsin *et al.,* 2019). Several gaps of blockchain technology were listed out by Jian-Foo and Swee-Huay (2022), such as absence of loops structures, Turing incomplete and longer time for blocks creations which are not in support of transactions in blockchain networks. Advert of Ethereum conveniently help to improve the block creation time; enabling developer to write smart contracts for Blockchain platforms and make it possible to customize Blockchain towards anticipated applications. Therefore, Ethereum compromises the chance of configuring IoT devices and privacy preservation in managing authentication operation for public key infrastructure (Grima *et al.,* 2021; Viriyasitavat *et al.,* 2019: Sanjekar and Patil, 2022) that have equal rights of different domains (Badlani *et al.,* 2022) without single point of failure (false tolerance) (Shrivastava *et al.,* 2019).

However, if existing anti-quantum signature schemes, such as lattice-based signature are used directly in blockchain to solve the problem, it would have made the wallet bloat. Therefore, anti-quantum transaction authentication schemes for blockchain are evolving for the purpose of constructing lightweight nondeterministic wallets, the key point is that public and private keys are generated from a set of master public and private keys (Seed Key). Hence, data stored (device) on the Permissioned Blockchain from concluded transactions needs small resources for protections since Blockchain system architecture is capable to provide necessary security clarifications for the entire IoT system.

Research Methodology

The vulnerability of data layer in MLS is protected adequately through appropriate permissioned access scheme. Cryptography enables the encryption the sensitive attributes of learner profile information, which is, scrambling of the sensitive attributes after packing them into blocks. The blocks are interconnected together using encryption/hashing values of previous blocks. The traditional hashing scheme is SHA-256 but, susceptible to Sybil and collision attacks, which informed the introduction of larger size and signing functions (Mohsin *et al.,* 2019). The PBS is a permission blockchain with higher privacy of sensitive attributes of learners' privacy data such as Matric/Registration Number, Date of Birth, Contact address,

Cumulative Grade Point Aggregates (CGPA), Medical Records, Web browser, Mobile Number, IP Address, Geolocation Data and Browsing History in the cloud (repository). The sensitive learners' attributes privacy preserving operations (cryptography, distributed ledger technology, and authentication and verification processes) of the PBS are presented in Algorithm 1 (Muhammad, 2024). Using Ethereum platform conveniently help to improve the block creation time; enabling developer to write smart contracts for Blockchain platforms and make it possible to customize Blockchain towards anticipated applications.

The privacy of MLS depends on the level of access control, data generated, learner profile information, and learning content. These components of MLS are susceptible to attacks and prone to privacy breaches and compromises. The use of appropriate keys, and informed consent approaches offered by permissioned blockchain that empowers the learners and administrators to enforced privacy of learners' data, and content use in MLS. Therefore, Ethereum compromises the chance of configuring IoT devices and privacy preservation in managing authentication operation for public key infrastructure that have equal rights of different domains without single point of failure (false tolerance) (Muhammad, 2024). The cryptosystem is used to secure non-sensitive attributes of the learner's location and personal data. Similarly, the sensitive component are protected using permissioned blockchain's hashing or cryptographic scheme for authorisation and access on the basis of lattice cryptography in order to enforce restricted access by undue users as depicted in Algorithm 1.

Algorithm 1

Algorithm 1: Learners' Data Privacy Preserving Algorithm

Input: Learners' profile information from the ODL system's database, Gj

Output Protected components of the learners' data, G,. P, S, p, s;

1. for every learners' data node, Gj,

2. for each learner's data parameter, W_g^f do

3. fetch the set of learner's data parameters, G_j, h

$G_j = \cup_{i=1}^{n} hu\ ,\quad 0 \le i \le n$ and $h1 * u1 + h2 * u2 + \ldots\ldots\ldots\ldots + hn * un$

4. Initialize learner's data parameters in step 3.

5. Identify the sensitive attributes in the learners' data;

6. where,

7.

8. $$W_g^f = G_j \frac{\omega}{c} \quad \Rightarrow\Rightarrow W_g^f = \bigcup_{i=1}^{n} Gj \frac{\omega}{c} \quad \Rightarrow\Rightarrow \bigcup_{i=1}^{n} \frac{\omega}{c} Gj$$

9.

10. Implement cryptographic algorithms (e.g., AES, RSA) to encrypt the

11. sensitive attributes:

12. for each S, D_e, H_r and e, r do

13. $$S\left[T_p\left(W_g^f\right)\right] = \begin{cases} D_e, & 128 \le e \le 256 \\ H_r, & 128 \le r \le 256 \end{cases}$$

14.

15. end for

16. divide the encrypted learner profile data into blocks and compute

17. cryptographic hashing values for each block to ensure data integrity, do

18. end for

19. end for

20 set up a permissioned blockchain network or use an existing one.

17. for each learners' sensitive data P, Z ,β_l^k , and k, l are the parameters; do

18. implement step 12 smart contracts to handle privacy operations ,

19. $$P\left[T_p\left(W_g^f\right)\right] = Z + v + \beta_l^k$$

20. end for

21. introduces a hashing cryptosystem offered by blockchain scheme to protect the privacy of private data of learner(s) do
22. for each initialized parameter in learners' sensitive data, T, in $(T_p(W_g^f)$then, apply PBC do
23. end for
24. implement an authorization mechanism to control access to sensitive attributes stored on the blockchain, P, S
25. for each sensitive attributes parameters P , S , p, s
26. as depicted in $\overrightarrow{P \otimes S} = (p \odot s)$,
27. develop an access control mechanism and Integrate the authorization process with the blockchain's smart contracts do
27. end for
28. prepare the output with privacy-preserved learners' data and Display the output to authorised parties as "privacy-preserving operations is successful" PBC, P, S, p, s; do
29. return PBC, $P, S)$ to store and control access to learners' sensitive data.

Results and Discussion

The relative performances of the proposed hashing schemes against traditional hashing schemes in creating blocks and chains for LDPPS are presented in Table 2.

Table 2: The average encryption time of hashing schemes compared outputs

Hashing Scheme	Elapsed Time (ms)
Proposed scheme (AES+SHA-1+Base64)	3889
SHA-1	1159
SHA-224	1349
SHA-256	1229
SHA-384	1208
SHA-512	1015
Bcrypt	33419
PBE	28657

From Table 2, the time taken for the proposed hashing scheme is relative simpler when compared to high-performing hashing schemes such as BCrypt and P-PBS-E due to rigorous process of forging hash values. The graphical representation of the various hashing scheme performances is shown in Figure 1.

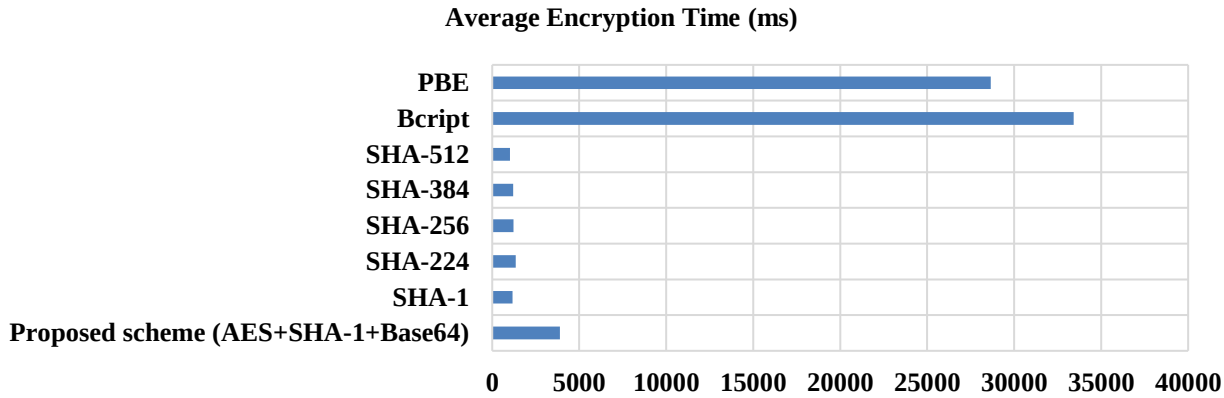

Figure 1: The average encryption time of hashing schemes compared outputs.

The relative performances of the proposed hashing schemes against traditional hashing schemes in creating blocks and chains for PBS are presented in Table 4.

Table 3: Performance of PBS using hashing schemes compared outputs

S/N	Hashing Scheme	PBS runtime(ms)	Hashing value size (bits)
1	Proposed scheme (AES+SHA-1+Base64)	4271	64
2	SHA-1	1984	40
3	SHA-224	1929	56
4	SHA-256	3693	64
5	SHA-384	3025	96
6	SHA-512	2301	60
7	BCrypt	39304	128
8	PBE	29769	156

Similarly, the hashing values sizes for the proposed scheme were smallest after SHA-1, SHA-224, SHA-512 against BCrypt and P-PBS-E schemes, which have the largest hashing value sizes. However, the level of security and scalability offered by the proposed scheme is comparable to the BCrypt and P-PBS-E schemes due to mode of operations required for generating blocks and associated hashes accordingly. The graphical representations are the PBS using the selected hashing schemes are illustrated in Figures 2 and 3.

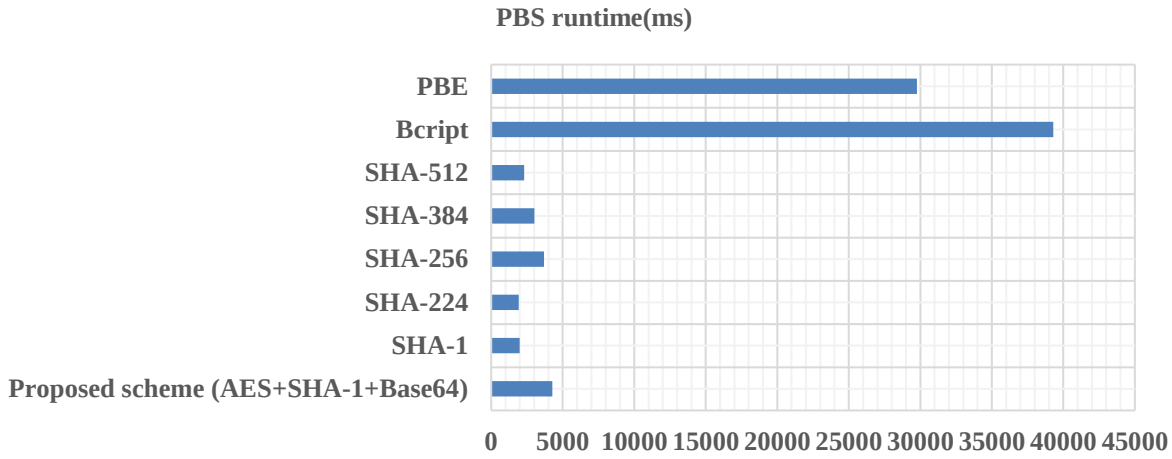

Figure 2: PBS runtime compared outputs.

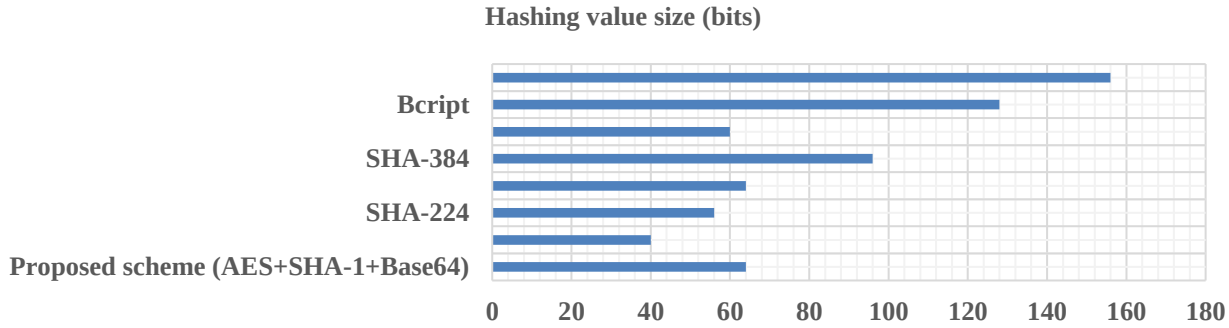

Figure 3: PBS hashing value sizes compared outputs.

Discussion

The results show that, using metrics such as encryption time, hash value size, and run-time (processing time) relatively outperformed existing approaches. The encryption time of the proposed hashing scheme (3889ms) was better than SHA-1 (1159ms), SHA-224 (1349ms), SHA-256 (1229ms), SHA-384 (1208ms), and SHA-512 (1015ms) in terms of offering effective privacy of learner sensitive profile information. When compared to the high-performing hashing schemes, the proposed hashing scheme was relatively secure against BCrypt (33419ms), and PBE (286567ms), which are indicative of complexity and security status of the proposed hashing scheme. Though, the hash value size of the proposed hashing scheme (64-bits) was better than SHA-1 (40-bits), SHA-224 (56-bits), SHA-256 (64-bits), SHA-384 (96-bits), SHA-512 (60-bits), BCrypt (128-bits), and PBE (156-bits) in terms of the scalability of the hashing schemes.

Similarly, on the BLPS-Chain runtime (or processing time), the proposed hashing scheme (4.95%) was higher than SHA-1 (2.30%), SHA-224 (2.23%), SHA-256 (4.28%), SHA-384 (3.51%), and SHA-512 (2.67%) for processing time. Conversely, the proposed hashing scheme trailed behind high-performing hashing schemes: BCrypt (45.56%), and PBE

(34.50%), which revealed that, higher runtime values offered better privacy of information on the blockchain technology influenced by extended hashing algorithms operations and functions.

Conclusion

Mobile Learning System is facing new challenge of privacy and data integrity due to the cloud backbone. The majority of the data exchanged concerns the learners' location and personal data. This further echoed the need for adequate security tool in e-learning environments to forestall present and future issues. Therefore, this work attempted to develop an appropriate access and authorization scheme based on blockchain technology for preserving privacy of LMS.

The results show that, using metrics such as encryption time, hash value size, and run-time (processing time) relatively outperformed existing approaches. On the Permissioned Blockchain Scheme (PBS) runtime (or processing time), the developed hashing scheme (4.95%) was higher than SHA-1 (2.30%), SHA-224 (2.23%), SHA-256 (4.28%), SHA-384 (3.51%), and SHA-512 (2.67%) for processing time. Conversely, the proposed hashing scheme trailed behind high-performing hashing schemes: BCrypt (45.56%), and PBE (34.50%), which revealed that, higher runtime values offered better privacy of information on the blockchain technology influenced by extended hashing algorithms operations and functions.

Future Work

In future works, the effectiveness of hashing scheme for blockchain authorisation and verification can be enhanced with stronger cryptographic schemes.

References

Ahmed, Y. A., Ahmad, M. N., Ahmad, N., & Zakaria, N. H. (2018). Social media for knowledge-sharing: A systematic literature review. *Telematics and Informatics*. https://doi.org/10.1016/j.tele.2018.01.015

Aldiab, A., Chowdhury, H., Kootsookos, A., Alam, F., & Allhibi, H. (2019). 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. https://doi.org/10.1016/j.egypro.2019.02.186

Ali, S., Islam, N., Rauf, A., & Din, I. U. (2018). Privacy and security issues in online social networks. *Future Internet*, *10*(114), 1–12. https://doi.org/10.3390/fi10120114

Alier, M., Casañ Guerrero, M. J., Amo, D., Severance, C., & Fonseca, D. (2021). Privacy and e-learning: A pending task. *Sustainability (Switzerland)*, *13*(16), 1–17. https://doi.org/10.3390/su13169206

Aly, M., Khomh, F., Haoues, M., Quintero, A., & Yacout, S. (2019). Enforcing security in internet of things frameworks: AC US CR. *Internet of Things*, 100050. https://doi.org/10.1016/j.iot.2019.100050

Atasoy, E., Bozna, H., & Abdulvahap, S. (2020). *Active learning analytics in mobile : Active visions from PhD students*. *15*(2), 145–166. https://doi.org/10.1108/AAOUJ-11-2019-0055

Avella, J. T., Kebritchi, M., Nunn, S. G., & Kanai, T. (2016). Learning analytics methods , benefits , and challenges in higher education: A Systematic Literature Review. *Online Learning*, *20*(2), 13–29.

Badlani, S., Aditya, T., Maniar, S., & Devadkar, K. (2022). EduCrypto: Transforming education using blockchain. *Proceedings - 2022 6th International Conference on Intelligent Computing and Control Systems, ICICCS 2022*, 829–836. https://doi.org/10.1109/ICICCS53718.2022.9788237

Bashari, B., Akbarzadeh, N., Ataei, P., & Khakbiz, Y. (2016). Security and privacy challenges in big data era. *International Journal of Control Theory and Applications*, *9*(43), 437–448.

Bernacki, M. L., Greene, J. A., & Crompton, H. (2019). Mobile technology, learning, and achievement: Advances in Understanding and measuring the role of mobile technology in education. *Contemporary Educational Psychology*, 101827. https://doi.org/10.1016/j.cedpsych.2019.101827

Cantabella, M., Martínez-españa, R., Ayuso, B., Yáñez, A., Muñoz, A., Cantabella, M., & Mart, R. (2018). big data framework Analysis of student behavior in Learning Management Systems through a Big Data framework. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.08.003

Cao, C., & Zhu, X. (2021). Trusted data management for e-learning system based on blockchain. *2021 IEEE 13th International Conference on Computer Research and Development Trusted*, 91–94.

Caviglione, L., & Coccoli, M. (2020). *A Holistic model for security of learning applications in smart cities*. *16*(01), 1–10. https://doi.org/10.1016/j.chb.2018.03.004

Djeki, E., Dégila, J., Bondiombouy, C., & Alhassan, M. H. (2022). E-learning bibliometric analysis from 2015 to 2020. *Journal of Computers in Education*. https://doi.org/10.1007/s40692-021 -00218-4

Esmaeilzadeh, P. (2018). The effects of Public concern for information privacy on the adoption of health information exchanges (HIEs) by healthcare entities the effects of public concern for information privacy on the adoption of health. *Health Communication*, 1–10. https://doi.org/10.1080/10410236.2018.1471336

Goswami, P. (2017). A survey on big data & privacy. *preserving publishing techniques*. *10*(3), 395–408.

Grima, S., Kizilkaya, M., Sood, K., & ErdemDelice, M. (2021). The perceived effectiveness of blockchain for digital operational risk resilience in the european union insurance market sector. *Journal of Risk and Financial Management*, *14*(8), 363. https://doi.org/10.3390/jrfm14080363

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, *97*, 512–529. https://doi.org/10.1016/j.future.2019.02.060

Hima, R., Kandakatla, R., & Gulhane, A. (2021). Role of learning analytics to evaluate formative assessments: Using a data driven approach to inform changes in teaching practices. *Journal of Engineering Education Transformations*, *34*, 550–556.

Jian-Foo, L. & Swee-Huay H. (2022). Secure file storage on cloud using hybrid cryptography *Journal of Informatics and Web Engineering, 1(2).*

Jones, K. M. L. (2019). *Learning analytics and higher education: A proposed model for establishing informed consent mechanisms to promote student privacy and autonomy*.

Juhanak, L., Zounek, J., & Rohlíkov, L. (2017). Computers in human behavior using process mining to analyze students ' quiz-taking behavior patterns in a learning management system. *Computers in Human Behavior Journal*, 1–11. https://doi.org/10.1016/j.chb.2017.12.015

Karthikeyan Nagaraj, (2023). Secure Hash Algorithm 1 (SHA-1): A comprehensive overview properties, applications, and vulnerabilities of SHA-1

Ketthari, M. T., & Rajendran, S. (2019). Privacy preserving data mining using hiding maximum utility item first algorithm by means of grey wolf optimisation algorithm. *International Journal of Business Intelligence and Data Mining*, *14*(3), 401–418.

Marjit, U., & Kumar, P. (2020). Towards a Decentralized and distributed framework for open educational resources based on IPFS and blockchain. *2020 International Conference on Computer Science, Engineering and Applications, ICCSEA 2020*. https://doi.org/10.1109/ICCSEA49143.2020.9132841

Mohanrao, M., & Karthik, S. (2019). Privacy preserving for global data using ensemble approach. *International Conference on Computer Vision and Machine Learning*, *1228*, 1–7. https://doi.org/10.1088/1742-6596/1228/1/012046

Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Albahri, A. S., Alsalem, M. A., & Mohammed, K. I. (2019). Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. *Computer Standards and Interfaces*. https://doi.org/10.1016/j.csi.2018.12.002

Muhammad, K. M. (2024). Development of permissioned blockchain based learners' data privacy preserving scheme in mobile learning system. PhD Thesis submitted to department of computer science, Federal University of Technology, Minna, Niger State - Nigeria.

Muhammad, K. M., Oyefolahan, I. O., Olaniyi, O. M., and Adebayo, O. J. (2023). Fuzzy analytic hierarchy process-based learner profile sensitive attributes determination in learning management system. Ilorin Journal of Computer Science and Information Technology, Department of Computer Science, University of Ilorin, Vol. 6, No. 1 (2023), ©ISSN: 2141-3959 *(print).*

Nagaraj, K., Sharvani, G. S., & Sridhar, A. (2019). Encrypting and preserving sensitive attributes in customer churn data using novel dragonfly based pseudonymizer approach. *Information*, *10*(274), 1–21.

Niknam, S., Dhillon, H. S., & Reed, J. H. (2019). Federated learning for wireless communications: Motivation , Opportunities and Challenges. *ArXiv:1908.06847v3*, 1–6.

Normadhi, N. B. A., Shuib, L., Nasir, H. N., Bimba, A., Idris, N., & Balakrishnan, V. (2018). Identification of personal traits in adaptive learning environment: Systematic literature review. *Computers & Education*. https://doi.org/10.1016/j.compedu.2018.11.005

Prinsloo, P., Khalil, M., & Slade, S. (2021). Learning analytics in a time of pandemics: Mapping the field. *European Distance and E-Learning Network (EDEN) Proceedings*, 60–70.

Revathi, A., Kaladevi, R., Gayathri, A., & Manju, A. (2021). Customized learning model using learner activity analysis. *Webology*, *18*, 607–618. https://doi.org/10.14704/WEB/V18SI04/WEB18152

Salman, T., Member, S., Zolanvari, M., Member, S., Erbad, A., Jain, R., & Samaka, M. (2019). Security services using blockchains: A state of the art survey. *IEEE Communications Surveys & Tutorials*, *21*(1), 858–880. https://doi.org/10.1109/COMST.2018.2863956

Sanjekar, R. D., & Patil, B. M. (2022). Techniques of securing educational document using blockchain and iPFS based system: A Review. *2022 International Conference for Advancement in Technology, ICONAT 2022*. https://doi.org/10.1109/ICONAT53423.2022.9726032

Sarker, N. I., Wu, M., Cao, Q., Alam, G. M. M., & Li, D. (2019). Leveraging digital technology for better learning and education: A systematic literature review. *International Journal of Information and Education Technology*, *9*(7), 453–461. https://doi.org/10.18178/ijiet.2019.9.7.1246

Shrivastava, A. K., Vashistth, C., Rajak, A., & Tripathi, A. K. (2019). A Decentralized way to store and authenticate educational documents on private blockchain: *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques, ICICT 2019*. https://doi.org/10.1109/ICICT46931.2019.8977633

Singh, H., & Miah, S. J. (2019). Design of a mobile-based learning management system for incorporating employment demands: Case context of an Australian University. Education and Information Technologies, 24(2), 995–1014. https://doi.org/10.1007/s10639-018-9816-1

Sivadanam, Y. L., Ramaguru, R., & Sethumadhavan, M. (2022). Distributed ledger framework for an Adaptive university management system. *Lecture Notes on Data Engineering and Communications Technologies*, *99*, 295–306. https://doi.org/10.1007/978-981-16-7182-1_24/COVER

Vatsaraj, V., Shah, J., Verma, S., & Dholay, S. (2021). *Decentralized document holder using blockchain*. 1–5. https://doi.org/10.1109/ICCCNT51525.2021.9579823

Viriyasitavat, W., Anuphaptrirong, T., & Hoonsopon, D. (2019). Journal of industrial information integration when blockchain meets internet of things: Characteristics , challenges , and business opportunities. *Journal of Industrial Information Integration*, (May), 0–1. https://doi.org/10.1016/j.jii.2019.05.002