SENSITIVITY OF LEARNERS' PRIVACY DATA (LPD) IN MOBILE LEARNING SYSTEM: A FUZZY ANALYTIC HIERARCHY SCHEME (FAHS) SOLUTION

MUHAMMAD KUDU MUHAMMAD, ISHAQ OYEBISI OYEFOLAHAN, OLAYEMI MIKAIL OLANIYI, OJENIYI JOSEPH ADEBAYO, ADEPOJU SOLOMON ADELOWO SALIU ADAM MUHAMMAD AND AYOBAMI 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, Abuja, Nigeria
Department of Cyber Security, National Open University, Abuja, Nigeria
Department of Cyber Security, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria
Email: Muhammad_kudu@futminna.edu.ng **Phone No:** +2348030594142

Abstract
Mobile technologies give room for possibilities of regular monitoring of learner's behaviour in order to establish proper user privacy protection. In educational system, safeguarding and free flow of administering of learners' privacy protection is key factor in learners' location and personal data. Learner's preferences, goals are important to achieve assessment by teachers' and smooth relationship among learners and create compromised preserving learners' privacy. To this end, learners' sensitive data in the cloud big data are exposed to sub-consciousness, stalking and theft. Therefore, the article addresses the issues of sensitivity among the learners' sensitive attributes such as personal and mobile devices data that enrolled in Mobile Learning System. However, attributes sensitivity solution using Fuzzy Analytical Hierarchy Schemes are being explored for the use of learners' profile due to the real danger from the Internet usage. Hence, concerns about sensitivity of learners' privacy data motivated this paper to adopt attributes partitioning strategy into sensitive and non-sensitive attributes ranging from 1 to 5 enforce privacy during learner profile information. Comparison between learners' data and mobile devices, shows that medical records as learners' data has FAHS weight of 0.9940 and APH weight of 0.0811 with highest sensitivity of 5 as most sensitive learners' private data. While browsing history as mobile devices has FAHS weight of 0.7861 and APH weight of 0.1471 with highest sensitivity of 5 as most sensitive mobile device. This implies that, these most/highest sensitive data/devices are vulnerable and must be protected to avoid privacy breaches, stalking, abuses, theft, sub-consciousness, harassments, and undue advantages of learners. In future works, preserving the privacy of sensitive MLS learners' privacy data sensitivity can be performed in a permissioned blockchain environment of Ethereum platform. The contributions / findings of the study were that, the article identifies learners' data sensitivity in Online Distance Learning/Mobile Learning System (ODL/MLS). The method determined learners' privacy data sensitivity in mobile learning system ranked the selected attributes using by relative importance index (RII) and as a results of this determination the private (privacy) of learners' data is preserved. The provide solution to privacy problems in MLS for effective access control and authorisation scheme through ownership of certain digital identity (DI) accessing various ODL services and platforms.

Key words: Attributes, Data, Learners', Sensitivity, Privacy, Analytical Hierarchy Process, Fuzzy Analytical Hierarchy Scheme

Introduction
In recent development, numerous institutions of learning are adopting mobile applications to offer services and carryout learning processes, which has created a phenomenon called mobile learning (m-learning) (Almaiah & Al Mulhem, 2019; Reidenberg & Schaub, 2018). Safeguards

for privacy are essential for the use of big data in education (Yacobson *et al.,* 2021). Digital identity (DI) in order to access authentication processes. DI systems represent the basic part of digital infrastructure that enables users to access authentication systems. Due to the existing multiple identities, the possibility of misuse and theft become high (Korac *et al.,* 2021). For several decades, learner authentication has been a cornerstone in online learning information systems (such as m-learning) (Mohsin *et al.,* 2019).

In quest to track learners' live location at any point in time during COVID-19 control initiative of The Albion College Michigan was laudable, but, the concerns about exposing personal and health related data of learners were held within the research community (Alier *et al.,* 2021). Efforts are put in place in order to protect users' data harvested through operations from third party users or apps integrated by default into the system for the purpose of data-sharing and mining (Merceron, 2015). Consequently, privacy concerns are more pronounced with online based data aggregation, storage and usages because the present-day age of information enables the invasion of private space of users through information collected by Information and Communication Technology (ICT) equipment in the intention to time, distance, location and maximize interactions (Rahman *et al.,* 2020).

Distance learning, whether synchronous or asynchronous mode, is attracting interests because of reachability and accessibility provided for human digital educational system. The use of mobile devices is considered valuable in improving human interaction educationally. Again, these devices collect learners' and learning analytics data which are valuable for the complete process of learning and other personalised services. Multi-criteria decision making theories of analytical hierarchy process, and the simple additive weighting models were proposed by (Saikat *et al.,* 2021) to assist in determining sensitive attributes of learner's data and mobile devices such as Matric/registration number, date of birth, contact address, Cumulative Grade Point Aggregate (CGPA), medical records, web browser, mobile number, IP address, location data and browsing history (Krumm *et al.,* 2021).

In particular, mobile learning platforms collect sensitive attributes about the learners in which geolocation information are integrated to enable various learning engagements including: movement/position tracking, class/lecture attendance, help and advisory services, social and interpersonal relationships operations within the study centres (Kabassi and Alepis,2020; Hongbo *et al.,* 2020). Learners' are uninformed about these activities in m-learning systems. Researchers and stakeholder have continued to argue about privacy risks and perceived consequences on the learners' well-being (Jones*,* 2019; Kambourakis, 2016). However, the real danger from the Internet use is in the lack of security and privacy. For the use of any e-learning platforms, learners have to own digital identity (DI) in order to access authentication processes. DI systems represent the basic part of digital infrastructure that enables users to access authentication systems. Due to the existing multiple identities, the possibility of misuse and theft become high (Adee and Mouratidis, 2022).

M-learning has the capability to assume a strong position in delivering a quality education in conjunction with the traditional approaches. This offers a customised, reliable and guaranteed dynamic computing setting for all participants (Korac *et al.,* 2021). It possible to infer location and personal data of learners' by crowd sourcing applications, which put severe risks on sensitive location and personal data privacy (Mohsin *et al.,* 2019). M-learning technologies have revolutionised the information access and models for educational purposes. Presently, knowledge is obtainable online, generally free, and simply accessible. Sharing, reading, listening and, performing are present-day skills necessary for education. Undoubtedly, mobile devices have become a complete set of applications, support, and help for educational organisations (Adee and Mouratidis, 2022). Research have indicated the individual are willing to provide comprehensive information of self to organisation with adequate security in place against third party exploitation or misuse such as Banks, Telecommunications and government agencies.

Often, privacy loss is an increasing phenomenon because majority of enterprises collect data of individuals in the bid to serve them better without recourse to implicit or explicit privacy loss concerns such as conducting investigations in fraud activities, abuse and wastages of funds in government establishments. But, the accuracy of personal information provided by individuals are in doubt because of safety of online based systems including mobile learning platforms. According to (Khan *et al.,* 2020) investigated on privacy leakage of multiple sensitive attributes correlation along-side with linkable sensitive bucket and generalisation table (GT) using privacy preserving data publishing (PPDP) of (c, k) - anonymization algorithm which yield an improved solution. However, the work reduces privacy risks with increased utility in general table, which is a threat for privacy measures. 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 Figure 1.

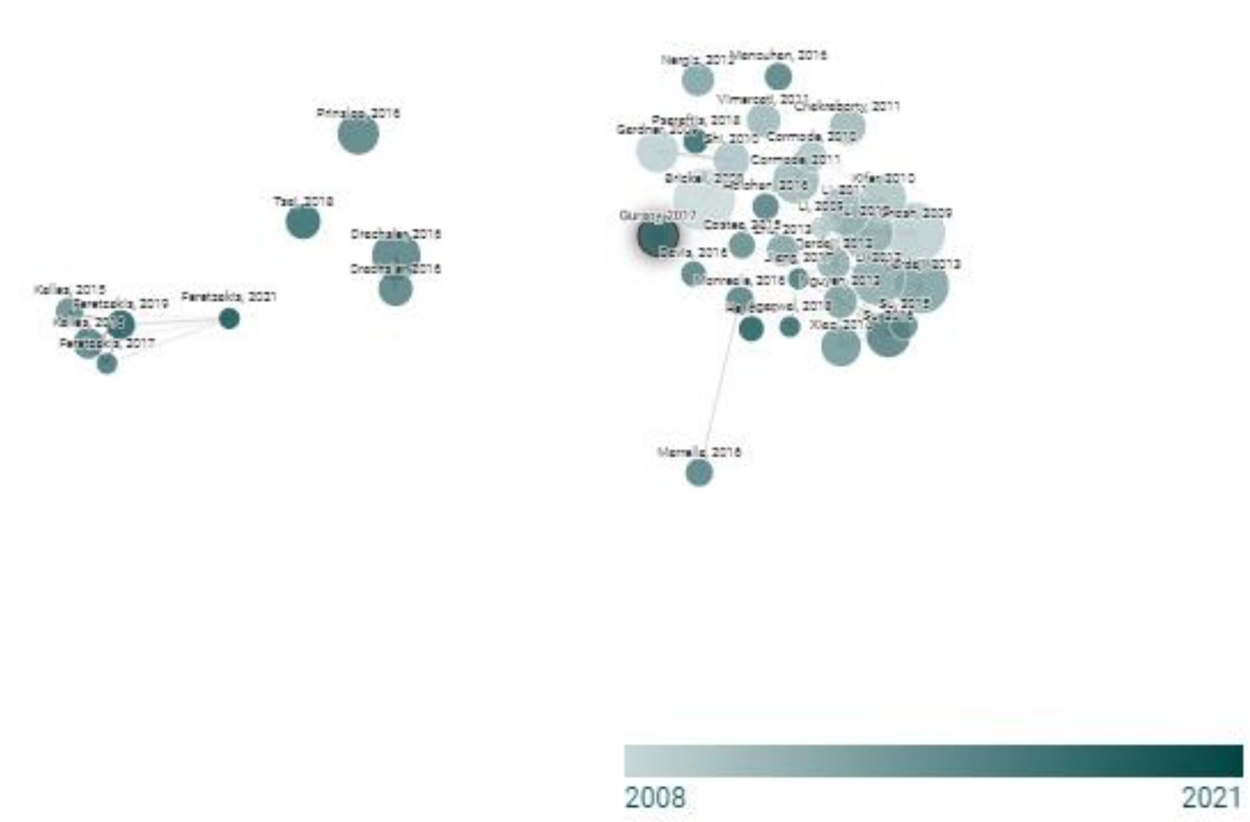

Figure.1: Efficient Privacy Preserving Scheme for Learners' Data and Mobile Devices Connected Papers, Source: Muhammad *et al.,* (2023)

Figure.1, the research included studies outside of the scope of the mapping article especially including post-2021 era. The article 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. The present research study is an attempt to make a contribution towards improving the privacy preservation of learner(s) profiles in mobile learning environment (m-learning) in Nigerian institutions. The research study evaluated analytically some sensitive attributes such as

Matric/registration number, date of birth, contact address, CGPA, health records, web browser, mobile number, IP address, geolocation data and browsing history (Kambourakis, 2013) for proper privacy protection (Shonola & Joy, 2014) of m-learner(s) data in a Nigerian institution.

Statement of the Problem

Learners' data is vulnerable to breaches on cloud storage or public repositories due to their sensitivity and presence of the personally identifiable information (PII) (Adee & Mouratidis, 2022). However, mobile learning platforms indirectly gather sensitive mobile devices and personal data especially location related such as Web Browser, Mobile number, IP Address, Geolocation data and, Browsing History whose privacy is not guaranteed (Hongbo *et al.,* 2020; Kambourakis, 2013). Therefore, m-learning systems have geo-location features to assists learners in diverse engagements such as movement and position tracking, lectures and classroom attendance and learning diagnosis, which is often available to advisors.

Related Studies

The use of learning technology has transformed the classical face-to-face learning situations and the acceptance of open and distance learning as augmenting traditional learning systems (Kambourakis, 2016). One main importance of m-learning into learning and teaching practices is the concept of learning analytics, which targets use of new tools to improve learning and teaching activities. M-learning analytics measures, collect, analyze and report big data concerning learners for the purpose of understanding and optimizing learning and learning situations (Kambourakis, 2016; Adee & Mouratidis, 2022). 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 (Kambourakis, 2016; Khan *et al.,* 2020; Kambourakis, 2013). The future works are to consider the best ways of performing involving operations in learners' data without fear of privacy compromises (Shonola and Joy, 2014; Atasoy *et al.,* 2020). There is need to determine the private elements of learner's data using machine learning algorithms alongside appropriate privacy preservation approaches. In this way, learner(s) should be able to give permission on request during learning analytics operations of educators or education service providers and by this, the privacy of the learner is preserved (Shonola & Joy, 2014).

Twelve articles on privacy preservation schemes/techniques such as K-anonymity, Blockchain techniques, Distributed authentication scheme, Private and public keys scheme, Anonymisation techniques, Encryption/Cryptography techniques, Randomisation/Noise addition, Perturbation techniques, Peer to Peer Network distributed scheme, Secured Multiparty Computation scheme and Virtual identity are major techniques used on learners' profile interms of privacy preservation in Online Distance Learning Cernters' and Moblie Learning System (MLS). A survey or systematic literature review on privacy preserving techniques were considered using the following metrices: such as title, author, year of publication, focus, methods, limitation, strength and conclusion with future work. Table 1 shown analysis of the previous related works on privacy preserving schemes.

In Table 2, articles reviewed are classified in to five (5), such as Blockchain techniques related articles, K-anonymity and Anonymisation articles, Randomisation/Noise addition and Perturbation articles, Secured Multiparty Computation and Encryption/Cryptography articles, and Virtual identity article all on Privacy Preserving and Mobile Learning as a baseline papers of the research work. Four (4) articles for blockchain related techniques, three (3) articles for a survey/SLR on privacy preservation using anonymisation and k-anonymity papers, three (3) articles for privacy preserving and the remaining three (3) articles for mobile learning. In conclusion, out of twelve (12) articles analysed, only six (6) articles were used to have the research direction. The authors established the ideas of traditional methods of privacy preserving as compared with conventional schemes of solving privacy preserving in the field of educational domain. Main privacy issues/challenges in mobile learning system/Learning Management System is illustrated in the Figure 2.

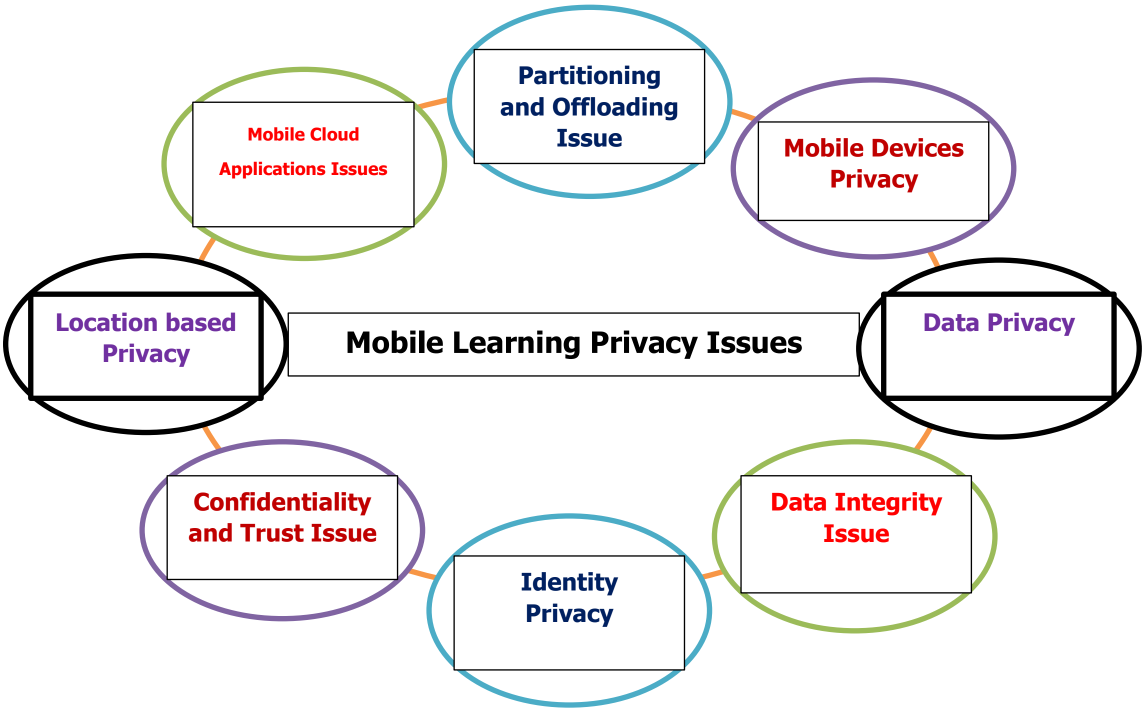

Figure 2: Mobile Learning Privacy Issues, Source: Muhammad, (2024)

By tracking, aggregating, and analysing student profiles along with students' digital and analog behaviours captured in MLS, educational institutions are beginning to open the black box of education using learning analytics technologies. Though, the increase in and usage of sensitive and personal student data present unique privacy concerns. In particular, location information can be useful for understanding behaviours of learners with potential of invading in individuals' privacy (Shonola & Joy 2014). Leading the race to providing privacy for educational big data is cryptography alongside granular access controls and data mining/operations (Ghouse & Anooj, 2015).

In educational big data, privacy is contemplated due to the real danger of the Internet. The mobile learning system harvest diverse digital identities about their learners, which are vulnerable to privacy compromises. Consequent upon this, this study proposed learners' location and personal attributes partitioning model to determine sensitive and non-sensitive attributes in learners' information repository (LIR). Then, privacy of these sensitive attributes is preserved from breaches.

Table 1: Privacy Preservations Schemes Related Work Analyses

S/No	Author(s)	Technique(s)	Strength(s)	Problem Identified/Weakness(es)	Remarks
1.	Ii and Osoba, 2017	Anonymisation	-Data storage, Data analysis, Data transfer. -Data acquisition, Rectifies record linkages.	-Attributes disclosure is high.	-Homogeneity and background attacks are common.
2.	Wang et al., 2018	Virtual identity	-Secure multi-party computation. -Better privacy protection.	-Scalability and information loss.	-Impracticable in educational setting due to learner information mining.
3.	(Jiang et al., 2018; Ram Mohan Rao et al., 2018; Zhao et al., 2020)	Encryption/ Cryptography	-High computational complexity. -Homomorphism	-Insufficient data utility. -Attribute disclosure.	-Cryptographic is superior to perturbation technique.
4.	Puneet and Suman, 2017	Perturbation	-Data noise addition, Random rotation. -Data modification, Confusion state is high. -Condensation, -Randomized responses.	-Slow and time inefficient.	-Geometric perturbation is more secure, than additive perturbation.
5.	Yin et al., 2018	Secure multi-party computation.	-Better than cryptography. -Data uselessness.	-Encryption is difficult to implement.	-Encryption reduces data importance during analytics.
6.	Salman et al., 2019	Randomisation	-No anonymisation cost. -Lesser computational overheads. -Add noise.	-Applicable to sentiment analysis. -Attributes disclosure is high.	-Data utility is minimized.
7.	(Zhou et al., 2018; Zhao et al., 2020)	K-anonymity	Masking of data by adding noise.	-Quality reduction, Storage inefficiency, -Homogeneity attacks. -Background attacks.	-Large storage and bandwidth requirements. -Attributes disclosure is pronounced.
8.	Zheng et al., 2017	Blockchain technology	-Transaction authentication based on ECDSA. -Cloud storage. -Tamper resistant.	-Vulnerable to imminent quantum attacks. -Identity authentication problems.	-Consideration for ant-quantum signature schemes. -Use of Seed key for public-private keys.
9.	Zhao et al., 2020	Distributed authentication	-Access control lists. -Data and resource providence. -Cloud computing paradigm.	-Services are prone to attacks.	-Decentralization overcomes privacy problems. -Data sovereignty with distributed ledger technology (DLT).
10.	Viriyasitavat et al., 2019	Peer-to-peer network of distributed nodes.	-Record of transactions are maintained across participating nodes. -Verification and validation.	-Vulnerable consensus mechanisms.	-Blockchain is secure by its design.
11.	Criollo-C et al., 2021	Public key and private key.	-Transactions are performed with private/public key. -No real identity exposure.	-Asymmetric cryptography are used to provide security for users and ledger consistency.	-Privacy/public keys strengths depend on under laying cryptography.
12.	Yin et al., 2019	Noise addition	-Randomization. -Shuffling, Reduce user record identity.	-Memory inefficient.	-Applicable for security of big data.
13.	Muhammad et al., 2023	Private key.	-Transactions are performed with private/public key.	-Cryptography used to provide privacy for learners' data in mobile learning environment.	-Private keys strengths depend on cryptography.
14.	Muhammad et al., 2024	Private key and blockchain technology.	-Transactions are performed with private key.	-Cryptography used to provide security learners' data and distributed ledger.	-Privacy keys strengths depend on cryptography.

Research Methodology

The article study gathered 3114 responses from learners through online survey platform link as (http://www.mkmphdlearnersprofilesystem.com/admin/manage-users.php) (Muhammad *et al.,* 2023) using physical extraction/online extraction that copied raw data files from a storage device directly from a live system while it is still in operation (real-time data replication) to the data collection approach by (Hima *et al.,* 2021 & Lwande *et al.,* 2021). The article chose random sampling technique for the choice of respondents from the learners' population due to dissimilarity of opinions on data elements sensitivity across distance learning centres and learning situations. The outputs of learner(s) Reponses on sensitivity attributes for location and personal data are in the results and discussion section. The learners' location and personal data form is designed using the samples collected from various institutions.

These samples were studied and extracted through a pilot study of Federal University of Technology, Centre for Online Distance e-Learning (CODe_L), Minna, Niger State-Nigeria. The extracted form is redesigned in to data structure such as personal characteristics, family circumstance, course (s) registration, previous knowledge, previous skills, mobile learning circumstances, user(s) details, fees payment and credentials, that contains thirty six (36) general learners' attributes. Out of these, after pilot study, nineteen (19) find to be among sensitive and non-sensitive attributes and later reduced to ten (10) attributes (Ji *et al.,* 2018 and Muhammad, 2024), after through observations from the learners' and other user(s) in Online Distance Learning (ODL) particularly (m-learning) centres. To collect the perception of learners and online distance learners on sensitivity of information volunteered during location and personal data privacy creation process (Zheng *et al.,* 2017). Firstly, the online survey respondents are except to provide responses based for five (5) Likert scale including: Most Sensitive = 5, More Sensitive = 4, Normal = 3, Less-Sensitive = 2, Non-Sensitive = 1. Base on the online questionnaire structure and its contents used shows in Table 2.

Table 2: Online questionnaire sample (Muhammad et al., 2023)

Question/Attributes	Learners' Data	Matric/Registration Number	Date of Birth	Contact Address	CGPA	Medical Records	Web Browser	Mobile Number	IP Address	Geolocation Data	Browsing History
Q1.	**Matric/Registration Number**										
Q2.	**Date of Birth**										
Q3.	**Contact Address**										
Q4.	**CGPA**										
Q5.	**Medical Records**										
Q6.	**Web Browser**										
Q7.	**Mobile Number**										
Q8.	**IP Address**										
Q9.	**Geolocation Data**										
Q10.	**Browsing History**										

The method that has been recognized as the most useful for researchers in meeting this objective is the Analytic Hierarchy Process-AHP (Soleimani & Lee, 2021). The Analytic Hierarchy Process (AHP) is a MCDA method of measurement through pair wise comparisons to derive priority scales based on the judgements of experts (Kubler *et al.,* 2016). The AHP has produced relatively effective decision-making in complex problems that are dealing with several criteria. Especially in supporting those type of decisions, which are resulted from collections of expert knowledge/preferences of decision-makers gathered usually by questionnaire forms.

Therefore, the AHP has been commonly used in various fields such as spatial decision support systems; traffic management or project risk assessment. Consequently, several studies have attempted to bring the results of AHP closer to real-life situations by integrating this model with other models such as fuzzy logic (Obiria *et al.,* 2015).

In the customary AHP, the pair shrewd examinations for each level concerning the objective of the best elective choice are directed utilizing a nine-point scale (Adepoju *et al.,* 2020). In this way, the utilisation of Saaty's AHP has a few inadequacies as in (Kutlu *et al.,* 2021). Variation of AHP, called Fuzzy AHP, originates into usage so as to defeat the compensatory method and the weakness of the AHP in dealing with etymological factors (Saaty, 2008). The fuzzy AHP scheme permits a more precise depiction of the dynamic decision cycle. The fuzzy AHP strategy can be seen as an unconventional scientific technique created from the customary AHP. By and large, it is difficult to mirror the decision uncertainty inclinations through fresh qualities.

Consequently, FAHP is used to soothe the uncertainness of AHP strategy, where the fuzzy correlations proportions are utilized. (Kambourakis, 2016; Al-Shammari & Mili, 2019; Adepoju *et al.,* 2020): presents another methodology for taking care of pair-wise examination scale dependent on triangular (three-sided) fuzzy numbers surveyed by utilisation of degree investigation technique for engineered degree estimation of the pairwise correlation. The initial phase in this technique is to utilize three-sided fuzzy numbers for pairwise correlation by methods for FAHP scale, and the following stage is to utilize degree investigation strategy to get need loads by utilizing engineered degree esteems (Al-Shammari & Mili, 2019).

Model Formation

The level of vagueness in human inclination covered with fuzzy sets in the pairwise examination during the AHP design. FAHP (AHP variant) was introduced to overcome the compensatory technique, and the AHP shortfalls in handling etymological cases (Saaty, 2008). Saaty, 2008 started the pair-wise investigation scale based on triangular (three-sided) fuzzy sets as highlighted in (Al-Shammari and Mili, 2019). Therefore, the learners' privacy data sensitivity (LDPS) model using FAHP steps are described as follows:

Assumption 1: Learning operations entails the process of collecting, measuring, analysing and reporting data on learners and their learning contexts for the purpose of understanding and improving the learning situation and environment. In MLS, the data and the data generated are advantageous to the instructor, learners' and educational managers, as well as malicious individuals.

Assumption 2: Recently, with the widespread adoption of MLS; it is possible to access data on the behaviours of learners. There is the prospect of classifying these data with educational data mining approaches and to transform them into visual information with learning operations. There is an increasing interest in the use of learning analytics for educational purpose.

Assumption 3: The extent of use of learners' location and personal data privacy needs to be investigated to protect sensitive and private data by instructors, managers and third-party agents.

Assumption 4: The new challenge for MLS is privacy considerations of learners' location and personal data, content and learning activities of principal actors. The process of developing mathematical model is grouped into three phases as discussed in the next subsections.

Step 1: Firstly, the paper formulated a pairwise fuzzy matrix on the basis of the selected learner privacy data sensitivity including: Matric/Registration Number, Date of Birth, Contact address, Cumulative Grade Point Aggregates (CGPA) and Medical Records, Web Browser, Mobile Number, IP Address, Location Data and Browsing History.

Where, ASI = attribute sensitivity index of learner privacy information, and rated privacy attributes PAi based on the ith attribute.

The outcomes of implementing the Privacy Preserving Scheme (PPS) to determine learners' privacy data sensitivity using the FAHP are described as follows:

Step 2: Firstly, the study developed a pairwise fuzzy comparison matrix based on relative importance index (RII) determined from learners profile. These includes: Matric/ Reg. Number, Browsing History, Biometric and Grade, Genotype, Geolocation Data, Medical Records, Personal Data, Mobile Number, IP Address, and Contact Address. The pairwise fuzzy comparison matrix was constructed using crisp numeric values indicated in next section.
RII = ΣW / (A*N)
1
Where,
W is the weighting given to each factor by the respondents (ranging from 1 to 5),
A is the highest weight, and N is the total number of respondents.

$$FSM = \begin{array}{c} PA1 \\ PA2 \\ PAx \\ PAZ \end{array} \begin{bmatrix} (1,1,1) & (a12, b12, c12) & (a1w, b1w, c1w) & (a1y, b1y, c1y) \\ (a21, b21, c21) & (1,1,1) & (a2w, b2w, c2w) & (a2y, b2y, c2y) \\ (ax1, bx1, cx1) & (ax2, bx2, cx2) & (1,1,1) & (axy, bxy, cxy) \\ (az1, bz1, cz1) & (az2, bz2, cz2) & (azw, bzw, czw) & (1,1,1) \end{bmatrix} \quad 2$$

Where FSM is fuzzy matrix, PA is learner privacy attributes of both location and personal, a is lower fuzzy number, b is median fuzzy number, c is upper fuzzy number.

Results and Discussion

The foremost level determines the sensitive attributes of learners' location data and mobile devices. Then second level analysed potential sensitive attributes in learners' profile information and by third level that developed the AHP comparison matrix before transforming into fuzzy triangular scale as in Table 3.

Table 3: Learners' Data and Mobile Devices Sensitivity FAHP - AHP Models Compared

Attribute/Criterion	FAHP	AHP
Matric / Registration Number	0.4156	0.1531
Date of Birth	0.4252	0.3612
Contact Address	0.4667	0.3354
CGPA	0.4672	0.2958
Medical Records	0.5430	0.2554
Web Browser	0.5481	0.3409
Mobile Number	0.5519	0.4512
IP Address	0.5869	0.2521
Geolocation Data	0.6023	0.2344
Browsing History	0.6500	0.3301

From Table 3, two models were compared, that is Fuzzy Analytic Hierarchy Process and the traditional Analytic Hierarchy Process model to check the ranking correlation sensitivity (weight) among the learners' location and personal attributes in mobile learning environment. This is represented in Figure 3.

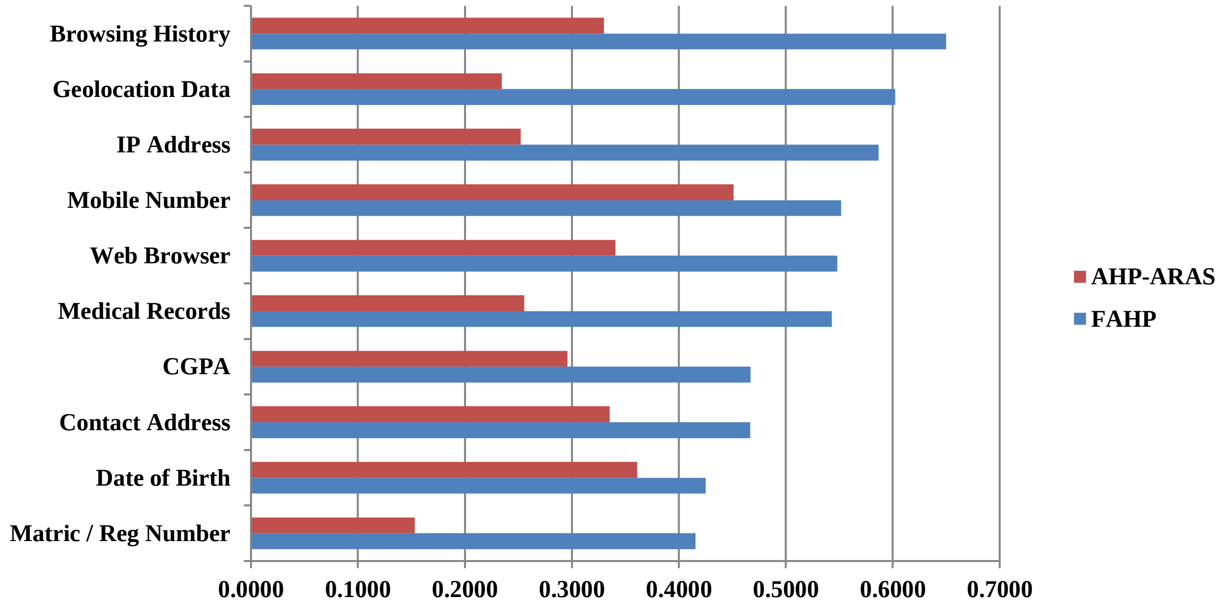

Figure 3: Learners' data and mobile devices sensitivity for FAHP-AHP compared

Table 4: Learner's Data Sensitivity FAHP Model

Attribute/Criterion	Weights	Sensitivity
Matric / Registration Number	0.3188	2
Date of Birth	0.1323	1
Contact Address	0.7678	4
CGPA	0.5983	3
Medical Records	0.9940	5

From Table 4, shows Fuzzy Analytic Hierarchy Process model to check the ranking correlation sensitivity (weight) among the learners' personal attributes in mobile learning environment.

Table 5: Learners' data Sensitivity for AHP Model

Attribute/Criterion	Weights	Sensitivity
Matric / Registration Number	0.6801	2
Date of Birth	0.9581	1
Contact Address	0.1769	4
CGPA	0.3723	3
Medical Records	0.0811	5

From Table 5, Traditional Analytic Hierarchy Process model to check the ranking correlation sensitivity (weight) among the learners' personal attributes in mobile learning environment.

Table 6: Learners' Data Sensitivity FAHP - AHP Models Compared

Attribute/Criterion	FAHP	AHP
Matric / Registration Number	0.3188	0.6801
Date of Birth	0.1323	0.9581
Contact Address	0.7678	0.1769
CGPA	0.5983	0.3723
Medical Records	0.9940	0.0811

From Table 6, two models were compared, that is Fuzzy Analytic Hierarchy Process and the traditional Analytic Hierarchy Process model to check the ranking correlation sensitivity (weight) among the learners' personal attributes in mobile learning environment.

Table 7: Learners' Mobile Devices Sensitivity FAHP Model

Attribute/Criterion	Weights	Sensitivity
Web Browser	0.4760	1
Mobile Number	0.5924	3
IP Address	0.5648	2
Geolocation Data	0.6680	4
Browsing History	0.7861	5

From Table 7, shows Fuzzy Analytic Hierarchy Process model to check the ranking correlation sensitivity (weight) among the learners' mobile devices in mobile learning environment.

Table 8: Learners' Mobile Devices Sensitivity AHP Model

Attribute/Criterion	Weights	Sensitivity
Web Browser	0.5705	1
Mobile Number	0.4349	3
IP Address	0.3914	2
Geolocation Data	0.2297	4
Browsing History	0.1471	5

From Table 8, Traditional Analytic Hierarchy Process model to check the ranking correlation sensitivity (weight) among the learners' mobile devices in mobile learning environment.

Table 9: Learners' Mobile Devices Sensitivity FAHP - AHP Models Compared

Attribute/Criterion	FAHP	AHP
Web Browser	0.476	0.5705
Mobile Number	0.5924	0.4349
IP Address	0.5648	0.3914
Geolocation Data	0.683	0.2297
Browsing History	0.7861	0.1471

From Table 9, two models were compared, that is Fuzzy Analytic Hierarchy Process and the traditional Analytic Hierarchy Process model to check the ranking correlation sensitivity (weight) among the learners' mobile devices in mobile learning environment.

Discussion

The results were achieved by converting to fuzzy numbers and reciprocal values of both traditional analytic hierarchy process and fuzzy analytic hierarchy process outcomes indicated in Table 3. Then consider the weight of learners' personal data using both AHP and FAHP, and sensitivity (weight) outcomes shows that medical records ranked high (5) in Table 4 and 5. Comparing the two (2) models as the one that is more effective in determining the sensitivity (weight), the outcomes indicate FAHP medical records (0.9940) rated high in Table 6.

Similarly, consider the weight of learners' mobile devices using both AHP and FAHP, and sensitivity (weight) outcomes shows that browsing history ranked high (5) in Table 7 and 8. Comparing the two (2) models as the one that is more effective in determining the sensitivity (weight), the outcomes indicate FAHP browsing history (0.7861) rated high in Table 9.

Conclusion

Online education such as MLS needs a high degree of data protection and privacy. This further echoed the need for adequate security tool in m-learning environments to forestall present and future issues. Therefore, this research work attempted to develop an appropriate access and authorisation scheme based on fuzzy analytic hierarchy scheme (FAHS) solution for preserving privacy of learners' sensitive attributes enrolled in MLS. The solution to privacy problems of MLS is effective access control and authorisation scheme through ownership of certain digital identity (DI) for the purpose accessing various ODL services and platforms. Comparison between learners' data and mobile devices, shows that medical records as learners' data has FAHS weight of 0.9940 and APH weight of 0.0811 with highest sensitivity of 5 as most sensitive learners' private data. While browsing history as mobile devices has FAHS weight of 0.7861 and APH weight of 0.1471 with highest sensitivity of 5 as most sensitive mobile device. Sensitive attributes FAHS technique can further investigated alongside permissioned blockchain privacy preserving schemes to disallow undue access or compromise of private learners' data and mobile devices, learning content, and learning behaviours as future work.

Future work

In this article, sensitivity in term of privacy of learners' data and mobile devices used by learners' in ODL/MLS is determined ranked by RII tool. Furthermore, discussed and analysed the privacy preserving scheme that can be used in protecting these learners' information and discovered almost all these schemes can compromise due to some of their weaknesses. Therefore, proposing blockchain technique or scheme for improving the learners' data privacy preservations in mobile learning System environment.

References

Adee, A., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors,* 22(3), 1109.

Adepoju, S. A., Oyefolahan, I. O., Abdullahi, M. B., & Mohammed, A. A. (2020). Multi-criteria decision-making based approaches in website quality and usability evaluation: A systematic review. *Journal of ICT*, *19*(3), 399–436. https://doi.org/10.32890/jict2020.19.3.5

Al-Shammari, M., & Mili, M. (2019). A fuzzy analytic hierarchy process model for customers ' bank selection decision in the Kingdom of Bahrain. *Operational Research*. https://doi.org/10.1007/s12351-019-00496-y

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

Almaiah, M. A., & Al Mulhem, A. (2019). Analysis of the essential factors affecting of intention to use of mobile learning applications: A comparison between universities adopters and non-adopters. *Education and Information Technologies*, *24*(2), 1433–1468. https://doi.org/10.1007/s10639-018-9840-1

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

Criollo-C, S., Guerrero-Arias, A., Jaramillo-Alcazar, A., & Luján-Mora, S. (2021). Mobile learning technologies for education: Benefits and Pending Issues. *Applied Sciences*, 11(4111), 1–17.

Ghouse, Sharif, G. M., & Anooj, P. N., (2015). Privacy preservation in educational data mining [PPEDM]. *International Journal of Advanced Computational Engineering and Networking,* 3(10), 79-82.

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.

Hongbo J., Jie, L., Ping, Z., Fanzi Z, Zhu, X., & Arun, I. (2020). Location privacy-preserving mechanisms in Location-based Services: A comprehensive survey.*ACM Comput. Surv.* 54, (1), https://doi.org/10.1145/3423165

Ii, J. S. D., & Osoba, O. (2017). *Privacy preservation in the age of big data. A Survey.* 1–15.

Jiang, R., Lu, R., & Choo, K. K. (2018). Achieving high performance and privacy- preserving query over encrypted multidimensional big metering data. Future Generation Computer System. 78, 392–401.

Ji, Y., Zhang, J., Ma, J., Yang, C., & Yao, X. (2018). BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information Systems. *Journal of Medical Systems*, 26-36. https://doi.org/10.1007/s10916-018-0998-2

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

Kabassi, K., & Alepis, E. (2020). Learning analytics in distance and mobile learning for designing personalised software. In *Machine Learning Paradigms, Intelligent Systems Reference Library* (pp. 185–203). Springer International Publishing. https://doi.org/10.1007/978-3-030-13743-4

Kambourakis, G. (2013). 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. *International Journal of U- and e- Service, Science and 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*, 13, 4(6), 46-54.

Karle, T., & Vora, D. (2017). Privacy preservation in big data using anonymization techniques. *2017 International Conference on Data Management, Analytics and Innovation*, 340–343. https://doi.org/10.1109/ICDMAI.2017.8073538

Khan, R., Tao, X., Anjum, A., Sajjad, H., Malik, R., Khan, A., & Amiri, F. (2020). *Privacy Preserving for Multiple Sensitive Attributes against Fingerprint Correlation Attack Satisfying c -Diversity*.

Korać, D., Damjanović, B., & Simić, D. (2021). A model of digital identity for better information security in e-learning systems. *Journal of Supercomputing*, (Mdi). https://doi.org/10.1007/s11227-021-03981-4

Krumm, A. E., Boyce, J., & Everson, H. T. (2021). A collaborative approach to sharing learner. *Event Data*. 8(2), 73–82.

Kubler, S., Robert, J., Derigent, W., Voisin, A., & Le, Y. (2016). A state-of the-art survey and test bed of fuzzy AHP (FAHP) applications. *Expert Systems with Applications, 65*, 398–422. https://doi.org/10.1016/j. eswa.2016.08.064

Kutlu, F., Duleba, S., Moslem, S., & Aydın, S. (2021). Evaluating public transport service quality using picture fuzzy analytic hierarchy process and linear assignment model. *Applied Soft Computing Journal*, *100*, 106920. https://doi.org/10.1016/j.asoc.2020.106920

Lwande, C., Muchemi, L., & Oboko, R. (2021). Identifying learning styles and cognitive traits in a learning management system. *Heliyon*, *7*, e07701. https://doi.org/10.1016/j.heliyon.2021.e07701

Merceron, A. (2015). Educational Data Mining/Learning Analytics: Methods, tasks and current trends. *Proceedings of DeLFI Workshops*, 101–109.

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, U*niversity of Ilorin, 6(1).

Norbutayevich, J. T. (2023). The use of mobile learning applications in higher education institutes. *Advances in Mobile Learning Educational Research*, *3*(1), 610–620. https://doi.org/10.25082/AMLER.2023.01.010

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

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 .*

Puneet, G. and Suman, M. (2017), A Survey on big data and privacy preserving publishing techniques. *Advances in Computational Science and Technology*, 10(3), 395-408.

Rahman, H. U., Rehman, A. U., & Nazir, S. (2020). Privacy and security — limits of personal information to minimize loss of privacy 1. *Springer International Publishing. https://doi.org/10.1007/978-3-030-12385-7*

Ram Mohan Rao, P., Krishna, S. M., & Kumar, A. P. S. (2018). Privacy preservation techniques in big data analytics: A survey. *Journal of Big Data. (JBD,* http://doi.org/10.1186/s40537- 018-0141-8,1-12.

Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education, 16*(3), 263–279. https://doi.org/10.1177/1477878518805308

Saaty TL (2008) Decision making with the analytic hierarchy process. *International Journal of Services Sciences, 1, 83.*

Saikat, S., Dhillon, J. S., Fatimah, W., Ahmad, W., & Jamaluddin, R. A. (2021). A systematic review of the benefits and challenges of mobile learning during the COVID-19 Pandemic. *Education Sciences*, *11*(459), 1–14.

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

Shonola, S. A., & Joy, M. (2014). Mobile learning security issues from lecturers' perspectives: (Nigerian universities case study). *EDULEARN14 Proceedings*, 7081–7088.

Soleimani, F., & Lee, J. (2021). Comparative analysis of the feature extraction approaches for predicting learners progress in online courses: MicroMasters credential versus traditional MOOCs. *L@Scale 4: Perspectives from Europe and US (L@S'21)*, 151–159.

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*, 0–1. https://doi.org/10.1016/j.jii.2019.05.002

Wang, S., Poon, W., Farnadi, G., Horst, C., Thompson, K., Nickels, M., Dowsley, R., Nascimento, A. C. A., & Cock, M. De. (2018.). *VirtualIdentity: Privacy-preserving user profiling*. 1–8.

Yacobson, E., Fuhrman, O., Hershkowitz, S., & Alexandron, G. (2021). De-identification is insufficient to protect student privacy. *Journal of Learning Analytics*, *8*(2), 83–92. https://doi.org/10.18608/JLA.2021.7353

Yin, W. E. I., Wen, Q., Li, W., Zhang, H. U. A., & Jin, Z. (2018). An anti-quantum transaction authentication approach in blockchain. *IEEE Access*, *6*, 5393–5401. https://doi.org/10.1109/ACCESS.2017.2788411

Zhao, Y., Member, G. S., Zhao, J., & Yang, M. (2020). Local differential privacy based federated learning for internet of things. *4662*(c), 1–18. https://doi.org/10.1109/JIOT.2020.3037194

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*. https://doi.org/10.1109/BigDataCongress.2017.85

Zhou T. Z., Cai, B. X, Leye, W., Ming, Xu, and Yueyue C. (2018). Privacy preserving data recovery for mobile crowd sensing. Proc ACM Interact. Mob. Wearable Ubiquitous Technol. 2(3), 151-23. https://doi.org/10.1145/3264961