Learners' Privacy-Preserving Scheme for Ranking Data Sensitivity in Mobile Learning System

Muhammad Kudu Muhammad
Department of Computer Science
Federal University Technology
Minna, Nigeria
0000-0001-8568-0743

Olayemi Mikail Olaniyi
Department of Cyber Security
National Open University of Nigeria
Abuja, Nigeria
0000-0002-2294-5545

Francis Osang
Department of Computer Science
National Open University of Nigeria
Abuja, Nigeria
0000-0002-2111-5785

Ishaq Oyebisi Oyefolahan
Africa Centre of Excellence on Technology Enhanced Learning
National Open University of Nigeria
Abuja, Nigeria
0000-0002-0954-5774

Ojeniyi Joseph Adebayo
Department of Cyber Security
Federal University Technology
Minna, Nigeria
0000-0003-0707-4152

Idris Mohammed Kolo
Department of Computer Science
Federal University Technology
Minna, Nigeria
0009-0004-5161-4595

2024 International Conference on Electrical and Computer Engineering Researches (ICECER) | 979-8-3315-3973-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICECER62944.2024.10920349

***Abstract* -- Mobile Learning System (MLS) is facing new challenges in terms of privacy, such as data collection, storage, and sharing because of the core infrastructure and network that enables cloud computing services. Most of the data exchange in Mobile Learning System (MLS) require mandatory authorisation to allow access to the learners' information in the MLS. Therefore, this article attempts to rank learners' sensitive attributes stored in MLS. Thus, concerns about privacy breaches motivated this paper to adopt an attributes partitioning strategy into the sensitive attributes to enforce privacy during learners' profile information access. The article adopted the informed consent phenomenon to determine and formulate learners' data privacy attributes sensitivity using the Fuzzy Analytic Hierarchy Process (FAHP) Algorithm. Results from the implemented Learners' Privacy Preserving (LPP) Algorithm determined normalized weights of top-five rank-selected learners' sensitive data to include: Browsing History (1ST, Ranked), Geolocation Data (2ND, Ranked), IP Address (3RD, Ranked), Web Browser (4TH, Ranked), Medical Records (5TH, Ranked) and CGPA (10TH, Ranked) respectively. This indicates that these five most sensitive features are at risk and require protection to prevent privacy breaches, thus ensuring privacy preservation that prevents unauthorised access to learners' sensitive data in the mobile learning system environment. The ranking of sensitive data in this paper could serve as inspiration for future research work on mobile learning security to improve the privacy of sensitive attributes in MLS environment**

Keywords- Attributes, Data, Learners', Mobile Learning System, Partitioning, Privacy Preserving, Profile, Sensitivity

I. INTRODUCTION

The use of mobile learning has risen dramatically, which was neither expected nor anticipated. The challenges and benefits of such widespread usage are beginning to emerge gradually [1-2]. These include connectivity, cheating, profiling, privacy and security. When data are in active process or use, adversaries may attempt to tamper with such data so as to compromise the security and privacy of the student information system (SIS) [3-7]. The use of third-party platform by institutions undertaking online educational system has further compounded privacy issues such as leakage of information and loss of data. The current trends show that the techniques or approaches used to resolve the user behaviour and data privacy preservation of learner profiling system is not fully a guarantee against breaches yet. The adversaries and attackers are finding their ways to tamper with sensitive information of individuals, government, organisations, business applications and in particular the field of Education [3]. Hence, the need for an enhanced privacy preservation model, this should be able to yield result that helps to solve the challenges of data security and privacy in mobile learners' data applications. Therefore, data sharing and data privacy are pressing issues that need to be addressed among the stakeholders of educational institutions. Following are the article's main contributions:

a. A method for detecting learners' privacy data sensitivity in mobile learning system environment using fuzzy analytic hierarchy technique and ranked.

b. This new LPP Scheme is formulated mathematically for effectiveness, efficiency and reliability.

This article is organised as follows: Section II summarises the related works. Section III explains the methodology of LPP Scheme. Section IV presents the results and discussion. Conclusion and suggestion for future work are given in Section V.

II. RELATED WORK

Most of the time, mobile learning has the capability to assume a strong position in delivering quality education when used in conjunction with the traditional approaches. This offers customised, reliable and guaranteed dynamic computing settings for all participants. With the use of mobile learning facilities, it is possible to infer location and personal data of learners through crowd sourcing applications, which put severe risks on sensitive location and personal data privacy. Multi-criteria decision-making theories of analytical hierarchy process, and the simple additive weighting models were proposed by [2] to assist in determining sensitive attributes of learner's data and mobile devices such as Matric/registration number, date of birth, contact address, CGPA, medical records, web browser,

979-8-3315-3973-3/24/$31.00 ©2024 IEEE

Authorized licensed use limited to: CHONNAM NATIONAL UNIVERSITY. Downloaded on March 19,2025 at 14:32:02 UTC from IEEE Xplore. Restrictions apply.

mobile number, IP address, location data and Browsing history [3]. This approach is completely acceptable using weights of attributes for decision by various reasoning and the alternatives' ultimate scores. As a result, any hybrid MCDM model that is developed must satisfy the requirement of coherence with regard to the decision-making process' phases.

Indeed, mobile learning platforms collect sensitive attributes about the learners in which geolocation information are integrated to enable various learning engagements. These includes; movement/position tracking, class/lecture attendance, help and advisory services, social and interpersonal relationships operations within the study centres [4-7]. M-learning system is characterised as online learning system that has accessibility, immediacy, interactivity, context-awareness, permanence and majority of mobile devices are of lower cost and light in weight compared to desktop Personal Computers (PCs). The major classes of mobile devices for m-learning deployed for use in education process has implications on the feel of the m-learning environment. Examples of mobile devices include: Notebook Computers, Personal Digital Assistance (PDA), Tablet PC, Smart Phones, Cellular Phones, Global System for Mobile Communication (GSM).

Privacy safeguards are essential for the use of big data arising from different platforms in education [8]. Drawing inspiration from [9], Privacy preservation in mobile learning system refers to restriction on learners' data being observed by the self or distributed to other observers," with personal digital data interpreted as "the information about persons captured by any means and then encoded in digital format" [10]. Due to the existence of multiple identities, the possibility of misuse and theft becomes high [11]. Thus, ensuring the privacy preservation of learners' location and personal sensitive attributes, will increase the level of trust and confidentiality among the users being learner – to – learner or/and learner – to – instructor. Presently, knowledge is obtainable online, generally free, and simply accessible. Sharing, reading, listening and performing are present-day skills needed for education. Undoubtedly, mobile devices have become a complete set of applications, support, and help for educational organisations. Presentations of multi-criteria decision approach to solve the problem of selecting attributes within mobile learning environment is task demanding in terms of the learners' knowledge level and learning styles in order to provide the needed conducive learning environment [12-16].

In addition, data surveillance continues to pose privacy and security breaches of learners' digital profile. There are little efforts in protecting the personal information of learners. Thus, the increase in usage of learners' data present unique privacy concerns. In particular, location information can be useful for understanding behaviours of learners and also has the potential of invading in individuals' privacy. These concerns call for the engagement of cryptographic approaches and the blockchain based technology for granular access controls and data mining/operations [4-5, 17, 18-22]. In a related comparative analysis, ranking of sensitive data in MLS enhance security, improved learning experience and protect sensitive information during the informed multi-criteria decision-making [23-28].

III. METHODOLOGY

The research study developed a privacy-protected learners' data by detecting the sensitive attributes using the Fuzzy Analytic Hierarchy Process (FAHP) model shown in Figure 1. Multi-Criteria Decision-Making (MCDM) scheme are often employed in real-world scenarios to solve problems with numerous, disproportionate, and conflicting criteria and/or objectives. [29]. It is commonly applicable in various fields such as education, the military, engineering, supplier evaluation and selection [30]. Also, It is an evident requirement that the uncertainty of evaluations be included throughout the weight determination stage, then, fuzzy methodology is applied [31-32]. The approach that has been identified as the most efficient for researchers in achieving this objective is the Analytic Hierarchy Process (AHP) [33]. The AHP is a MCDA technique of measurement through pair wise comparisons to obtain importance scales based on the suggestions of experts and ranked the selected attributes by relative importance index (RII).

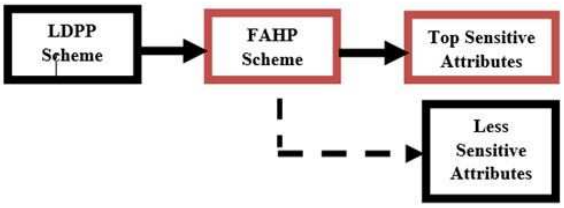

Fig. 1. Learners' Data Privacy Scheme [34]

The fuzzy assessment grid of the measures was built through the pairwise correlation that assigns relevant semantic factors and triangular fuzzy numbers. The reciprocal values obtained from fuzzy numbers led to attributes based linguistic values and judgment decision made by the respondents of the sampled institutions as crisp values shown in results and discussion Section.

Data files were copied from a storage device, regardless of the relationships between data components. It can be of two types: taking data straight from a live system while it is still in operation (real-time data replication) and extracting data from a system that is no longer running. The data collection for this study was collected through Google link/online survey from learners at different Online distance eLearning (ODeL) units in Nigeria Institutions. The survey harvested various information through physical extraction/online extraction in MLS of learners' data, content management, learning activities and assessment which is comparable to the data collection approach in the studies by [35-36].

The Google link was sent to learners at various Institutions (Centres) on Mobile Learning Programme across Nigeria. The institutions are Federal University of

Authorized licensed use limited to: CHONNAM NATIONAL UNIVERSITY. Downloaded on March 19,2025 at 14:32:02 UTC from IEEE Xplore. Restrictions apply.

Technology, (FUT) Centre for Online Distance eLearning (CODeL), Minna, National Open University of Nigeria (NOUN) Study Centres, University of Abuja Distance Learning Centre, Ahmadu Bello University, Distance Learning Centre, Zaria and National Teachers Institution (NTI) Open Distance Programme, North Central. Five Thousand and Five (**5005**) responses were received and validated. Learners' respondents that are valid across various Institutions are **3114** with **1891 as** invalid using Matric/Registration Number format by various institutions in Table I.

Table I. Distributed and Responses of Learners' from various Institutions

S/No.	Institutions	Learners' Responses	Valid Responses	Invalid Responses
1	FUT, Centre for Online Distance eLearning, Minna	405	65	340
2	NOUN Study centres,	1000	825	175
3	University of Abuja, Distance Learning Centre,	800	520	280
4	Distance Learning Centre, ABU Zaria	850	635	215
5	NTI Open Distance Programme, North Central	1950	1069	881
	Total Responses	**5005**	**3114**	**1891**

The details analysis of questionnaires distributed and responses of learners' that filled Google link from various Institutions selected as most learners' data sensitivity are in Table II.

Table II. Learners' Data Sensitivity

Attributes	N S	L S	N	M S	V S	Weighted sum	Total Number (N)	A*N	RII	RANK
Matric/Registration Number	91	212	4386	1332	5610	11631	3114	15570	0.750	7TH
Mobile number	67	152	192	2460	8530	11425	3114	15570	0.734	8TH
Date of birth	221	674	3660	388	5695	10638	3114	15570	0.683	9TH
Contact Address	70	182	3462	2120	6345	12179	3114	15570	0.782	6TH
Medical Records	103	210	549	4492	8000	13352	3114	15570	0.858	5TH
Browsing history	12	56	150	3696	10500	14414	3114	15570	0.926	1ST
CGPA	110	236	1530	2040	5140	9056	3114	15570	0.582	10TH
Web Browser	20	56	796	4760	8050	13682	3114	15570	0.879	4TH
Geolocation Data	22	34	213	3652	10455	14376	3114	15570	0.923	2ND
IP Address	20	76	246	4800	8870	14012	3114	15570	0.899	3RD

From Table II, Considering the ranking of sensitive data in terms of learners' responses; Browsing History recorded highest (10500) as the most sensitive attributes, and then followed by Geolocation data (10455); IP Address (8870); Web browser (8050); and Medical records (8000) respectively.

In FAHP, the focus of correct practices in terms of using pair comparison in each phase analysis is to accomplished by a 9-point scale [33], Saaty's AHP-MCDM approach. This addresses the level of vagueness in human inclination protected a sets of fuzzy numbers compare with pairwise to scrutinised the AHP scheme. FAHP scheme is presented to overcome the compensatory technique, and the AHP shortfalls in handling etymological cases [31]. The pair-wise evaluation scale is based upon triangular (three-sided) fuzzy sets as highlighted in [32]. Therefore, the Learners' Sensitive Data and privacy preserving scheme using FAHP steps are formulated mathematically as follows:

Step 1: The paper developed a hierarchy structure with distinct levels. The first level determines the sensitivity of the attributes of learners' location and personal data. The second level analysed potential Potentially, sensitive features in learners' data. The third level constructed a comparison matrix in an AHP prior to transitioning to a fuzzy triangular scale as selected sensitive attributes using 5-point scale and fuzzy numbers transformation scale alternatives (1, 3, 5, 7 and 9). The grid for assessing the fuzzy sets/representations is built via a pair-wise connection of unique attributes linked with overall subjects based on semantic parameters and triangular fuzzy [34].

Step 2: Firstly, the paper developed a pairwise fuzzy [25] matrix on the premise of the selected learners' sensitive attributes. Hence, Equation 1 depicted the Fuzzy Matrix developed. The result obtained after computation of fuzzy numbers gives its reciprocal values.

$$FSM = \begin{matrix} PA1 \\ PA2 \\ PAx \\ PAZ \end{matrix}\begin{bmatrix} (1,1,1) & (\tau 12, \delta 12, \partial 12) & (\tau 1w, \delta 1w, \partial 1w) & (\tau 1y, \delta 1y, \partial 1y) \\ (\tau 21, \delta 21, \partial 21) & (1,1,1) & (\tau 2w, \delta 2w, \partial 2w) & (\tau 2y, \delta 2y, \partial 2y) \\ (\tau x1, \delta x1, \partial x1) & (\tau x2, \delta x2, \partial x2) & (1,1,1) & (\tau xy, \delta xy, \partial xy) \\ (\tau z1, \delta z1, \partial z1) & (\tau z2, \delta z2, \partial z2) & (\tau zw, \delta zw, \partial zw) & (1,1,1) \end{bmatrix} \quad 1$$

Where FSM is fuzzy matrix, PA is learners' privacy attributes of both location and personal, r is lesser fuzzy number, δ is middle fuzzy number, ∂ is higher fuzzy number.

Step 3: The Fuzzy Geometric Mean (FSM^{gm}) is calculated for the FSM as given by Equation 2.

$$FSM^{gm} = \begin{bmatrix} V1\tau & V1\delta & V1\partial \\ V2\tau & V2\delta & V2\partial) \\ Vx\tau & Vx\delta & Vx\partial) \\ Vz\tau & Vz\delta & Vz\partial \end{bmatrix}; where\ V\tau, V\delta, V\partial = \begin{cases} V\tau = \left(\sum_{x=1}^{y} \tau zy\right)^{1/y} \\ V\delta = \left(\sum_{x=1}^{y} \delta zy\right)^{1/y} \\ V\partial = \left(\sum_{x=1}^{y} \partial zy\right)^{1/y} \end{cases} \quad 2$$

While, Vτ is lesser fuzzy geometric mean, Vδ is middle fuzzy geometric mean, V∂ is higher fuzzy geometric mean, and FSM^{gm} is the fuzzy geometric mean decision matrix.

Step 4: The calculation of Fuzzy Weight (Tw) is as shown in Equations 3 and 4.

$$Tw = \left(\frac{\sum_{x=1}^{y} V\tau}{\sum_{x=1}^{z}\sum_{w=1}^{y} Vz\tau}, \frac{\sum_{x=1}^{y} V\delta}{\sum_{x=1}^{z}\sum_{w=1}^{y} Vz\delta}, \frac{\sum_{x=1}^{y} V\partial}{\sum_{x=1}^{z}\sum_{w=1}^{y} Vz\partial}\right) \quad 3$$

Authorized licensed use limited to: CHONNAM NATIONAL UNIVERSITY. Downloaded on March 19,2025 at 14:32:02 UTC from IEEE Xplore. Restrictions apply.

$$Tw = (T\tau, T\delta, T\partial) \quad 4$$

Tw is Fuzzy Weight, Tτ, Tδ and T∂ are lesser, middle and higher fuzzy weight respectively.

Step 5: The computation of the Weight of attributes (Ww) in learners' data (Learners' location and personal data) is given by Equation 5

$$Ww = \frac{(Ta + Tb + Tc)}{3} \quad 5$$

Where, Ww is Weight of attributes in learners' data.

Step 6: Computation of Normalized Weight (Wn) of learner privacy attributes is given by Equation 6.

$$Wn = \frac{Ww}{\sum_{w=1}^{y}(Ww)} \quad 6$$

Hence, $w = 1, 2, \ldots, y$, Wn is Normalized weight

Learners' sensitive attributes were given a weighting value of 1 due to their identical importance, resulting in a single numeric value to categorize learners' privacy sensitivity. The last attributes sensitivity index (ASI) is given by Equation 7

$$ASI = \sum_{i=1}^{n}(Wn\ x\ PA) \quad 7$$

Therefore, ASI = Attribute Sensitivity Index of learners' privacy data, and rated privacy attributes PAi based on the ith attribute. The equations ranging from 1 to 7 transforms Learners' Privacy Preserving (LPP) Scheme.

IV. RESULTS AND DISCUSSION

The computation of the Weight of attributes (Ww) in learners' data is as depicted in Equation 5. The result in Table I led to the result in Table II. The details analysis of questionnaires distributed and responses of learners' that filled Google link from various Institutions are in Table III and IV. The equivalent weights of fuzzy numbers and their reciprocals are used to calculate the weights using the fuzzy geometric mean shown in Equation 2. This is presented in Table III as Institutions Crisp Values and Table IV are the learners' valid responses attracted to sensitive attributes from various selected mobile learning institutions.

Table III. Institutions Crisp Values

Institutions/ Attributes	Web Browser	Medical Records	IP Address	Geolocation Data	Browsing History
FUT, CODel	4	5	5	5	5
NOUN Study Centres	4	3	4	5	5
Abuja, DLC	5	5	4	5	4
ABU, DLC	4	4	4	4	4
NTI	3	5	5	4	5
Min/Max	5	5	5	5	5

From Table III, Institution crisp values are learner sensitive attributes response in five point scale, thus attributes have equal single numeric value for categorising learners' privacy attributes sensitivity and lead to Table IV.

Table IV. Weights for Learners' Sensitive Data by Institutions

Institutions/Attributes	**Web Browser**	**Medical Records**	**IP Address**	**Geolocation Data**	**Browsing History**
FUT, CODel	0.8	1	1	1	1
NOUN Stu. Centres	0.8	0.6	0.8	1	1
Abuja, DLC	1	1	0.8	1	0.8
ABU, DLC	0.8	0.8	0.8	0.8	0.8
NTI	0.6	1	1	0.8	1

From Table IV, the normalised weights of learners' sensitive attributes in Federal University of Technology, Centre for Online Distance eLearning (CODeL), Minna is higher according to learners' responses towards the sensitivity of attributes selected. Follow by University of Abuja Distance Learning Centre, then, National Teacher Institute (NTI) Open Distance Programme, North Central, National Open University of Nigeria (NOUN) Study centres and Ahmadu Bello University (ABU) Distance Learning Centre respectively shown in Figure 2.

Authorized licensed use limited to: CHONNAM NATIONAL UNIVERSITY. Downloaded on March 19,2025 at 14:32:02 UTC from IEEE Xplore. Restrictions apply.

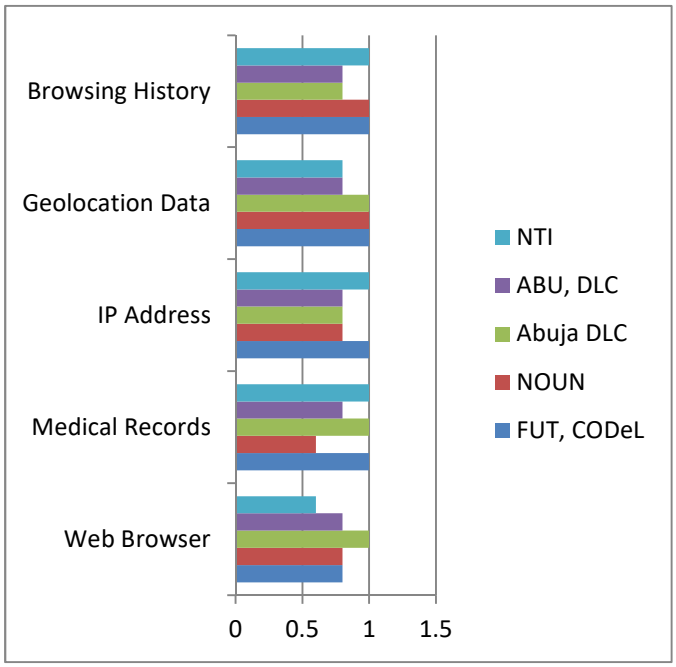

Fig. 2. Learners' Sensitive Data /Weights by Institutions

Similarly, fuzzy numbers from the crisp values of selected Institutions that are running distance learning programme. From Table VI, Fuzzy Analytic Hierarchy Process selected and ranked some attributes to be most sensitive attributes according to linguistic judgment and decision from learners' in various Mobile Learning System Environment mentioned above.

IV. CONCLUSION

Privacy preserving is anticipated to actually solve the problem of learners' data vulnerability in the Internet that make mobile learning system (MLS) environment secured, effective access control, high level of authentication and verification with authorisation. These are through ownership of certain digital identity (DI) for the purpose of accessing sensitive data in ODL platform. Learners' Data Privacy (LDP) Scheme approach determined the weights and ranked the sensitive attributes as followed; browsing history (1), followed by geolocation data (2), then, IP address (3), web browser (4) and Medical records (5) respectively. Finally, learners' data privacy scheme developed enhance security, increase learners' trust and protect sensitive information to denied undue access or compromise of private learners' data.

ACKNOWLEDGEMENT

Sincere thanks and appreciation go to the Africa Centre of Excellence on Technology Enhanced Learning and the National Open University of Nigeria (NOUN), Abuja for sponsoring the presentation of this paper at the 2024 International Conference on Electrical and Computer Engineering Research (ICECER 2024), Gaborone-Botswana.

REFERENCES

[1] A. E. Krumm., J. Boyce., and H. T. Everson, (2021). A Collaborative Approach to Sharing Learner Event Data. 8(2), *73*–82.

[2] K. Kabassi and E. Alepis (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.

[3] J. Hongbo, L. Jie, Z. Ping, Z. Fanzi, X. Zhu and I. Arun (2020). Location Privacy-preserving Mechanisms in Location-based Services: A Comprehensive Survey. *ACM Comput Surv.* 54, 1, Article 4 (December 2020), 36 pages, https://doi.org/10.1145/3423165

[4] M. Alier, M. J. Casañ Guerrero, D. Amo, C. Severance, and D. Fonseca (2021). Privacy and e-learning: A pending task. *Sustainability*, *13*(16), 1–17.

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

[6] G. Kambourakis (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.

[7] B. Chang (2020). *Privacy Issues in Online Learning Environment*. 27–31.

[8] J. R. Reidenberg and F. Schaub (2018). Achieving big data privacy in education. *Theory and Research in Education, 16*(3), 263–279.

[9] A. Pardo & G. Siemens (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology, 45*(3), 438–450.

[10] E. Yacobson, O. Fuhrman, S. Hershkowitz and G. Alexandron (2021). De-identification is insufficient to protect student privacy, or—What can a field trip reveal? *Journal of Learning Analytics*, *8*(2), 83–92.

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

[12] J. T. Norbutayevich (2023). The use of mobile learning applications in higher education institutes. *Advances in Mobile Learning Educational Research*, *3*(1), 610–620.

[13] Y. Zhao, G. S. Member, J. Zhao and M. Yang (2020). *Local Differential Privacy based Federated Learning for Internet of Things*. *4662*(c),1–18.

[14] S. Criollo-C, A. Guerrero-Arias, A. Jaramillo-Alcazar and S. Luján-Mora (2021). Mobile Learning Technologies for Education: Benefits and Pending Issues. *Applied Sciences*, *11*(4111), 1–17.

[15] P. Goswami (2017). *A Survey on Big Data & Privacy Preserving Publishing Techniques*. *10*(3), 395–408.

[16] S. Kubler, J. Robert, W. Derigent, A. Voisin & Y. Le (2016). A state-of the-art survey and test bed of fuzzy AHP (FAHP) applications. *Expert Systems with Applications, 65*, 398–422.

[17] S. A. Adepoju, I. O. Oyefolahan, M. B. Abdullahi and A. A. Mohammed (2020). Multi-Criteria Decision-Making Based Approaches in Website Quality And Usability Evaluation: A Systematic Review. *Journal of ICT*, *19*(3), 399–436.

[18] J. T. Norbutayevich, (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

[19] S. Badlani, T. Aditya, S. Maniar, & K. Devadkar (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

[20] R. D. Sanjekar and B. M. Patil (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.

[21] Y. L. Sivadanam, R. Ramaguru, and M. Sethumadhavan (2022). Distributed Ledger Framework for an Adaptive University Management System. *Lecture Notes onData Engineering and Communications Technologies*, *99*, 295–306. https://doi.org/10.1007/978-981-16-7182-1_24/COVER

[22] S. Ennouamani, Z. Mahani and L. Akharraz (2020). A context-aware mobile learning system for adapting learning content and format of

Authorized licensed use limited to: CHONNAM NATIONAL UNIVERSITY. Downloaded on March 19,2025 at 14:32:02 UTC from IEEE Xplore. Restrictions apply.

presentation: design, validation an evaluation. *Educ Inf Technol* 25, 3919–3955 (2020). https://doi.org/10.1007/s10639-020-10149-9

[23] K. Gulzar, O. Tariq, S. Mustafa, S. M. Mohsin, S. N. Kazmi, S. M. A. Akber, & M. Ali (2023). A fuzzy analytic hierarchy process for usability requirements of online education systems. *IEEE Access*

[24] I., Vinogradova-Zinkevič, (2023). Comparative sensitivity analysis of some fuzzy AHP methods. *Mathematics*, *11*(24), 4984.

[25] H. Li, L. Ge, & L. Tian. (2024). Survey: federated learning data security and privacy-preserving in edge-Internet of Things. *Artificial Intelligence Review*, *57*(5), 130.

[26] N. S. M. Zaki, J. Bidin, N. Sharif, K. A. K. Akil, & S. Nayan (2024). Fuzzy Analytic Hierarchy Process (FAHP) in Analyzing Mathematical E-Learning Success Factors. *Journal of Computing Research and Innovation*, *9*(2), 485-495.

[27] A. E. S. Freitas, L. A. Rodrigues, & E. P. Duarte Jr, (2024). VCubeChain: A scalable permissioned blockchain. *Ad Hoc Networks*, *158*, 103461.

[28] T. K. Vashishth & S. Chaudhary (2023). Privacy and Confidentiality in Permissioned Blockchain Networks: Evaluating Security Models. *Future Trends in Business: Knowledge, Skills, Sustainability, Innovation and Technology (FTB-KSSIT-2023)*, 45.

[29] F. Kutlu, S. Duleba, S. Moslem and S. Aydın (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

[30] T. L. Saaty (2008) Decision making with the analytic hierarchy process. International Journal of Services Sciences 1: 83.

[31] R. Eslamipoor (2022): A fuzzy multi-objective model for supplier selection to mitigate the impact of vehicle transportation gases and delivery time. *Journal of Data, Information and Management,* vol. 4, https://doi.org/10.1007/s42488-022-00076-4

[32] T. Chen and H.-C Wu (2020). Fuzzy collaborative intelligence fuzzy analytic hierarchy process approach for selecting suitable three-dimensional printers. *Soft Computing*. https://doi.org/10.1007/s00500-020-05436-z

[33] J. Yee, J. Ooi, Y. Kin, and V. Andiappan (2021) Synthesis of wastewater treatment process (WWTP) and supplier selection via Fuzzy Analytic Hierarchy Process (FAHP). *Journal of Cleaner Production*, *314*, 128104. https://doi.org/10.1016/j.jclepro.2021.128104

[34] M. K. Muhammad, I.O Oyefolahan, O.M. Olaniyi, and O.J. Adebayo (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).*

[35] R. Hima, R. Kandakatla, and A. Gulhane (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.

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

Authorized licensed use limited to: CHONNAM NATIONAL UNIVERSITY. Downloaded on March 19,2025 at 14:32:02 UTC from IEEE Xplore. Restrictions apply.