**Fuzzy Analytic Hierarchy Process-based Learner Profile Sensitive Attributes Determination in Learning Management System**

Muhammad Kudu Muhammad1\*, Ishaq Oyebisi Oyefolahan2, Olayemi Mikail Olaniyi3, Ojeniyi Joseph Adebayo4

*1Dept. of Computer Science, Federal University of Technology, Minna-Niger State, Nigeria,* *muhammad\_kudu@futminna.edu.ng*

*2Dept. of Information Technology, Federal University of Technology, Minna-Niger State, Nigeria,* *o.ishaq@futminna.edu.ng*

*3Dept. of Computer Engineering, Federal University of Technology, Minna-Niger State, Nigeria,* *mikail.olaniyi@futminna.edu.ng*

*4Dept. of Cyber Security, Federal University of Technology, Minna-Niger State, Nigeria,* *ojeniyia@futminna.edu.ng*

\* Corresponding author

# Abstract

# *Context: The concept of learning analytics is used for the purpose of aggregating, tracking, and scrutinising learner profiles using the digital and non-digital traits available in the Learning Management System (LMS). This is widespread with educational institutions as means of opening the potential of education through suitable analytics technologies. Recently, the openness of educational repositories to support learner profile learning analytics has raised issues of privacy due to access to sensitive information for diverse purposes. The opportunity to utilize learning technologies to be able to gather, analyze, and measure information about learners and learning environments, and process them into big data. To this end, learners’ private or sensitive attributes in the cloud big data are exposed to sub-consciousness, stalking and theft. Objective: Therefore, concerns about privacy breaches motivated this research to adopt attributes partitioning strategy into sensitive and non-sensitive attributes to enforce privacy during learner profiling using Fuzzy Analytic Hierarchy Process (FAHP) model. Method: This paper develops normalized weights and Attribute Sensitivity Index (ASI) computation index based on the FAHP model to determine top-five sensitive attributes in learners’ profile information. Ten (10) attributed were identified as most relevant for inclusion in the learner’s profile in which five (5) attributes were considered to be most-sensitive to respondents. Results: From these outcomes, top-five sensitive attributes in learner profile information were identified including: Marital Status (19.69%), CGPA (17.10%), Date of Birth (14.64%), Mobile number (14.21%), and Full Name (9.97%). Conclusion: This implies that, the top-five sensitive attributes 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 LMS learners’ profile information can be performed in a blockchain environment.*

**Keywords:** *Learning Management System, Learner Profile, Sensitive, Privacy Preservation, Fuzzy Analytical Hierarchy Process.*

# 1. Introduction

Majority of developing and advanced economics rely on education as foundation of all innovations. There is recent awareness about the connection between living or contributing to the society and education appreciations of individuals around the world. Basically, the traditional system of education is received through a face-to-face or one-to-one classroom approach. Higher education system mostly depends on cloud backbone as in the case of Learning Management System (LMS) or online class system, for the purpose of teaching and learning services outside of traditional classroom settings(Chatterjee, *et al.,* 2021).

The learning landscape for the 21st century student and academics has been positively turnaround by LMS.LMS has enabled both e-learning and online teaching resources to assist in self-space information collection and collaborative, and problem solving - related actions (Ferguson and Clow, 2017). Specifically, higher educational level (universities) has adopted the LMS to address shortfalls in the provision of learning management services to educators and learners within these institutions (Kabassi and Alepis, 2020).Again, LMS adoption improves the learning and teaching activities and administration, but, it is yet to have a lasting positive impact on pedagogy due to the insecurity of data harvested (Singh and Miah, 2018).

Present-days learning platforms leverage the interconnectedness within peoples, multimedia artifacts’, events, places, and things to offer smart services such as data, realistic hands-on laboratories, and learning stimuli. Though, the learning platforms propelled by smart systems are prone to several privacy and security issues due to reliance on IoT nodes, cyber-physical systems, and wireless sensor networks(Caviglione and Coccoli, 2020). Attackers can easily scrutinize transactions performed, actions, traffic information, and user location information for possible privacy and security breaches (Wang, *et al.*, 2019).

The progression in digital technology has given new meaning to data management, not merely the efficient storage and retrieval of data, but now includes the way of generating useful information from it. Recently, networking technologies have facilitated the gathering and distribution of an expansive quantity of data; thereby making the concept of distributed data mining a vital data management component. The constant usage of hardware and software systems/devices helps in improving diverse computing and exchanges. There is relatively storage ease, retrieval and processing big data (Ketthari and Rajendran, 2019).

Often, it is argued that, data mining in LMS can be performed securely as to preserve private information during customized learning processes. According to Mohanrao and Karthik, (2019), the educational sector has progressed in manner as to provide prospects for collecting and examining private information about learners to obtain valuable insights, not without grave dangers (Nagaraj, Sharvani and Sridhar, 2019). Traditionally, educational and learning management systems consume and harvest personal data and metadata of students, and operated by third-parties outside of host learning institutions. In the past five years, students’ information are reposed and managed without learning institutions controls(Alier, *et al.,* 2021). This approach exposes learners to privacy compromises, which is undertaken in this paper.

The paper contributes as follows:

1. A conceptual model for determining learners’ profiles sensitive and non-sensitive attributes in LMS;
2. Formulation of fuzzy analytic hierarchy process model for preserving sensitivity of learners’ profile information;
3. Validation of the proposed model;

This next presents the related works. Section three presents the research methodology and section four presents the results and their implications. Finally, the conclusion of the paper is presented in section five.

# 2. Review of Related Works

Privacy refers to the concern of individuals about revealing/protecting personal information of one’s own or other people. Though, prior studies have given little focus to privacy, in spite of its significance in the perspective of individuals and organizations. As the technology is developing day by day, the privacy of the information security became highly significant (Khan and Alshare, 2019).

LMS requires the convergence of the learners and learning platforms into an interactive environment enabled by portable devices, wireless sensors, and objects. There are sparingly scarce works done on trust, security and privacy problems of LMS (Caviglione and Coccoli, 2020). LMS is facing new challenge of privacy and data integrity due to the cloud backbone. The majority of the data exchanged concerns the user's personal information. The choice of suitable authorization regulations and procedures is largely challenging especially that there is the need to guarantee only authorized users have access to sensitive data (Chatterjee et al., 2021).

A number of these private sensitive data of learners have been identified including: name, gender, birth data, address, credit card details, biometric characteristics of a actors, mobile phone number, email address, nationality, work history, location data, IP address, IMEI, location data, service usage data, e-mail, call record and web-browsing log files and history, and security credentials (Mohanrao and Karthik, 2019; Atasoy et al., 2020; Turnbull, Chugh and Luck, 2020; Korac, Damjanovic and Simic, 2021).The rate of awareness of privacy and security in previous studies are summarized in Table **2.1**.

**Table 2.1: Summary of major related studies**

|  |  |  |  |
| --- | --- | --- | --- |
| S/N | Author(s) | Domain of study | Privacy and security considerations |
| 1. | ( Normadhi, *et al.,* 2018) | Adaptive e-learning system | -No mention.-It offers personalised learning environment and self-directed. |
| 2. | (Aldiab, *et al.,* 2019) | LMS | -No mention.-No mention. |
| 3. | (Alharthi, Spichkova, and Hamilton, 2018) | E-Learning Systems | -No mention. |
| 4. | (Cantabella, *et al.,*2018) | LMS | -Privacy of learners’ data elements.-Learner behavioural patterns. |
| 5. | (Garone, *et al.,*2019) | LMS | -No mention.-Mining of learners’ data.  |
| 6. | (Niknam et al., 2019) | Mobile Learning Systems | -Private data of actors or learners needs privacy protection. |
| 7. | (Antonius, *et al.,* 2019) | LMS | -No mention. |
| 8. | (Ahmed, Ahmad, Ahmad, and Zakaria, 2018) | Knowledge Sharing | -No focus on the impact of security and privacy concerns about platforms, and tools applicable for knowledge sharing. |
| 9. | (Sarker, *et al.,* 2019) | Digital Technology based learning and education | -No mention.-No mention. |
| 10. | (Revathi, *et al.*, 2021) | E-Learning | -Safeguards for learners’ private information. |
| 11. | (Atasoy, Bozna and Abdulvahap, 2020) | E-Learning | -Learner information and learning analytics breach privacy.-Possibility of stalking, theft and sub-consciousness.  |
| 12. | (Hima, Kandakatla, and Gulhane, 2021) | E-Learning | -Learning performance and feedback tools are privacy-prone. |
| 13. | (Prinsloo, Khalil, and Slade, 2021) | E-Learning  | -Feedback tool in LMS provides learner activities and personal information.-Security, ethics, and privacy issues are increasing.  |
| 14. | (Djeki, Dégila, Bondiombouy, & Alhassan, 2022) | E-Learning | -Security and privacy of data.-Learner and learning content protection. |

From Table **2.1**, there are still open issues about conducting safe learning analytics on LMS whose intention is to improve learning situations (such as security and privacy breaches) regardless of the obvious benefit of knowledge sharing (Ahmed et al., 2018).

A number of confirmations were available on the use of learners’ private data and behavioural activities by LMS especially in studying and understanding the needs of learners as well as improvement of their experiences.

The data assists in situating technology for educational purposes; but, technology increases in the risks of learners’ information on LMS(Cao and Zhu, 2021). Specifically, the privacy and security lapses caused by mining processes of learners were not considered by (Normadhi, *et al.,* 2018; Aldiab *et al.,* 2019; Sarker et al., 2019).

There is general consensus on the fact that learners’ behavioural patterns and personal data are often harvested by LMS during teaching and learning activities. Learner information mining is required for the proper functioning of LMS, but, legitimate use of learners’ data for providing better learning experiences cannot be guaranteed (Djeki *et al.,* 2022).

**3. Research Methodology**

**3.1 Conceptual Model of Learner Profile Scheme**

The Learner Profile Scheme (LPS) is formulated with sensitive attributes in learner profile information using FAHP, whose main components are represented in conceptual diagram illustrated in Figure **3.1**.



Figure **3.1:** The conceptual diagram of the Learner Profile Scheme.

From Figure **3.1**, the main components of the LPS are the input, process and output. The input to the model is the learner profile information generated from the field surveys. The process to the model is the composed of FAHP attributes sensitivity determination block. The sensitive attributes block, and the non-sensitive attributes block serve as output to the model. Thereafter, the entire attributes partitions can be protected on Blockchain. The procedure is further explained using mathematical definitions in the subsequent subsections.

**3.1.1 Fuzzy AHP**

In AHP, the pair comparison investigation of finest choice for every level of objective are conducted with a **9**-point scale (Kumar *et al.,* 2021). Saaty’s AHP-MCDM approach has few inadequacies including:

1. Best applied in new selection problems,
2. Well-suited for highly equal verdict sizes,
3. The AHP strategy doesn’t consider the vulnerability related with the planning of one’s judgment to a number,
4. Fairly loose ranking,
5. Leaders’ determination, expression, and inclination considerably affect judgment outcomes.

The level of vagueness in human inclination is covered with fuzzy sets in the pair-wise examination during the AHP design. FAHP (AHP variant)was introduced to overcome the compensatory technique, and the AHP shortfalls in handling etymological cases (Chen and Wu, 2020)

Chang (1996) started the pair-wise investigation scale based on triangular (three-sided) fuzzy sets as highlighted in (Yee, *et al.*, 2021). Therefore, the Learner Profile Attributes Sensitivity (LPAS) model using FAHP steps are described as follows:

Step **1**: AHP development. The paper developed a hierarchy structure with unique levels. The foremost level determines the sensitive attributes of learner profiling information. The second level analyzed potential sensitive attributes in learner profile information. The third level developed the AHP comparison matrix before transforming into fuzzy triangular scale as shown in Table **3.1**.

From Table **3.1, t**he grid for evaluating the fuzzy sets/representations is constructed by means of the pair-wise connection of distinct attributes associated with overall subjects based on semantic parameters and triangular fuzzy sets as shown in Figure **3.1**.

**Table 3.1: Crisp values conversion scale for survey Likert scale**

|  |  |  |  |
| --- | --- | --- | --- |
| Alternatives | Select sensitive attributes using 5-point scale | Fuzzy Numbers conversion scale | Alternatives |
| Non-sensitive | 1 | 1 | More of less equally important |
| Less-sensitive | 2 | 3 | Moderately more important |
| Normal | 3 | 5 | Strongly more important |
| More sensitive | 4 | 7 | Very strongly important |
| Most sensitive | 5 | 9 | Extremely more important |



Figure **3.1**: The crisp numeric values of scale of importance.

Step **2:** Firstly, the paper formulated a pair-wise fuzzy matrix on the basis of the selected learner profile attributes including: Full Name, Mobile Number, Date of Birth, Genotype, Contact Address, Medical Records, CGPA, Matric/ Reg. Number, Marital Status, and IP Address.

Therefore, the fuzzy matrix was developed as follows as expressed in Equation **3.1**. This is achieved by converting to fuzzy numbers and reciprocal values indicated in Table **4.1** whose outcomes are shown in Table **4.2**.

$$FSM= \begin{matrix}PA1\\PA2\\\begin{matrix}PAx\\PAZ\end{matrix}\end{matrix}\left[\begin{matrix}(1,1,1)\\(τ21,δ21,∂21)\\\begin{matrix}(τx1,δx1,∂x1)\\(τz1,δz1,∂z1)\end{matrix}\end{matrix}\begin{matrix}(τ12,δ12,∂12)\\(1,1,1)\\\begin{matrix}(τx2,δx2,∂x2)\\(τz2,δz2,∂z2)\end{matrix}\end{matrix}\begin{matrix}(τ1w,δ1w,∂1w)\\(τ2w,δ2w,∂2w)\\\begin{matrix}(1,1,1)\\(τzw,δzw,∂zw)\end{matrix}\end{matrix}\begin{matrix}(τ1y,δ1y,∂1y)\\(τ2y,δ2y,∂2y)\\\begin{matrix}(τxy,δxy,∂xy)\\(1,1,1)\end{matrix}\end{matrix}\right] (3.1)$$

where FSM is fuzzy matrix, PA is learner profile attributes, r is lower fuzzy number, δ is median fuzzy number, ∂ is upper fuzzy number.

**Step 3:** The fuzzy geometric mean is computed for the FSM as given by Equation **3.2**.

$$FSM^{gm}= \left[\begin{matrix}V1τ \\V2τ\\\begin{matrix}Vxτ\\Vzτ\end{matrix}\end{matrix}\begin{matrix} V1δ)\\V2δ\\\begin{matrix}Vxδ\\Vzδ\end{matrix}\end{matrix}\begin{matrix}V1∂\\ V2∂)\\\begin{matrix} Vx∂)\\Vz∂\end{matrix}\end{matrix}\right];where Vτ,Vδ,V∂= \left\{\begin{matrix}Vτ= \left(\sum\_{x=1}^{y}τzy\right)^{1/y}\\Vδ= \left(\sum\_{x=1}^{y}δzy\right)^{1/y}\\V∂=\left(\sum\_{x=1}^{y}∂zy\right)^{1/y}\end{matrix}\right. (3.2)$$

Vτ is lower fuzzy geometric mean, Vδ is medial fuzzy geometric mean,

V∂ is upper fuzzy geometric mean, and

$FSM^{gm}$ is the fuzzy geometric mean decision matrix.

**Step 4:** The computation of fuzzy weight is given by Equations **3.3** and **3.4**.

$$Tw= \left(\frac{\sum\_{x=1}^{y}Vτ}{\sum\_{x=1}^{z}\sum\_{w=1}^{y}Vzτ},\frac{\sum\_{x=1}^{y}Vδ}{\sum\_{x=1}^{z}\sum\_{w=1}^{y}Vzδ} , \frac{\sum\_{x=1}^{y}V∂}{\sum\_{x=1}^{z}\sum\_{w=1}^{y}Vz∂}\right) (3.3)$$

$$Tw =\left(Tτ, Tδ,T∂\right) (3.4)$$

Tw is fuzzy weight, Tτ, Tδ and T∂ are lower, median and upper fuzzy weight correspondingly.

**Step 5:** The calculation of the weight of attributes in learner profile information is given by Equation **3.5**.

$$Wn= \frac{Ww}{\sum\_{w=1}^{y}(Ww)} (3.6)$$

$$Ww=\frac{(Tτ+ Tδ+T∂)}{3} (3.5)$$

Where, Ww is Weight of attributes in learner profile information.

**Step 6:** Calculate normalized weight of learner profile attributes is given by Equation **3.6**.

Where, $w=1, 2, …,y$,

Wn is normalized weight

Learner sensitive attributes were given equal weight of 1 because the attributes have equal importance which depicts a single numeric value for categorizing learner profile attributes sensitivity. The final sensitivity index of learner profile information attributes is given by Equation **3.7**.

$$ASI= \sum\_{i=1}^{n}\left(Wn x PAi\right) (3.7)$$

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

* 1. Data Collection and Analysis

The non-availability of required data necessitated the use of online survey platform

**(http://www.mkmphdlearnersprofilesystem.com/admin/manage-users.php)** to collect the perception of learners and online distance learners on sensitivity of information volunteered during profile creation process(Chang, 1996). 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.** The online questionnaire structure and its contents are provided in Table **3.2**.

**Table 3.2: Online questionnaire structure**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | Learner profile attribute | Full Name | Mobile No. | Date of Birth | Genotype | Contact Address | Medical Records | CGPA | Matric/Registration No. | Marital Status | IP address |
| Q1. | **Full Name** |  |  |  |  |  |  |  |  |  |  |
| Q2. | **Mobile No.** |  |  |  |  |  |  |  |  |  |  |
| Q3. | **Date of Birth** |  |  |  |  |  |  |  |  |  |  |
| Q4. | **Genotype** |  |  |  |  |  |  |  |  |  |  |
| Q5. | **Contact Address** |  |  |  |  |  |  |  |  |  |  |
| Q6. | **Medical Records** |  |  |  |  |  |  |  |  |  |  |
| Q7. | **CGPA** |  |  |  |  |  |  |  |  |  |  |
| Q8. | **Matric/ Reg No.** |  |  |  |  |  |  |  |  |  |  |
| Q9. | **Marital Status** |  |  |  |  |  |  |  |  |  |  |
| Q10. | **IP Address** |  |  |  |  |  |  |  |  |  |  |

This article gathered **3114** responses from learners from the online survey platform composed learners, students and individuals from different Centre for Open Distance and eLearning (CODeL) units in Nigeria concerning the relative sensitivity of data elements supplied on e-learning management system, which comparable to the data collection approach by (Hima, Kandakatla, & Gulhane, 2021; Lwande, Muchemi, & Oboko, 2021). The paper chose random sampling technique for the choice of respondents from the students’ population due to dissimilarity of opinions on data elements sensitivity across LMS and learning situations.

* 1. Experimental Settings

The study utilised **3114** responses from randomly sampled respondents through the online survey platform for analysis larger than reported in (Lwande et al., 2021) that collected **311** log histories of learners who reasonably retrieved learning modules for a three months within same institution. The original datasets were prepared into Microsoft Excel **2016** format for ease of data processing in MATLAB R**2019**b environment. The minimum parameters for hardware and software are highlighted in Table **3.3**.

**Table3.3: Minimum experimental parameters.**

|  |  |
| --- | --- |
| Parameters | Values  |
| Hardware |  |
| HDD | 180GB |
| Processor speed | 2.0GB |
| System processor type | 64-bit |
| Processor name | AMD |
| Software |  |
| Operating system | Windows 8 |
| Discrete Simulator | MATLAB R2019b |
| Pre-processor | Microsoft Excel 2016 |

4. Results and Discussions

The outcomes of implementing the Learner Profile Scheme to determine Learner Attributes Sensitivity (LPAS) using the FAHP are described as follows:

The pair wise fuzzy comparison matrix was constructed using crisp numeric values indicated in Table **3.2** and Figure **3.1** as shown in Table **4.1**.

**Table 4.1: Fuzzy component chart for Chang 2020 method**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Attribute/Criteria | Full Name | Mobile Number | Date of Birth | Genotype | Contact Address | Medical Records | CGPA | Matric/Reg No. | Marital Status | IP Address |
| Full Name | 1 | 1/5 | 1/8 | 6 | 3 | 7 | 3 | 2 | 1/3 | 3 |
| Mobile Number | 0 | 1 | ¼ | 5 | 6 | 5 | 1/5 | 1 | 1/7 | 7 |
| Date of Birth | 0 | 0 | 1 | ¼ | 5 | 6 | 1/5 | 4 | 1 | 1/3 |
| Genotype | 0 | 0 | 0 | 1 | 1/3 | 4 | 1/6 | 7 | 1/5 | 1 |
| Contact Address | 0 | 0 | 0 | 0 | 1 | 1/3 | 1/7 | 5 | 1/4 | 4 |
| Medical Records | 0 | 0 | 0 | 0 | 0 | 1 | 1/4 | 1/5 | 1/5 | 8 |
| CGPA | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 7 | 1/4 | 1/9 |
| Matric/ Reg No. | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1/7 | 1/5 |
| Marital Status | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 7 |
| IP Address | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

Therefore, the study developed fuzzy matrix using the following matrix in Equation **3.1**. The pair-wise fuzzy matrix presented in Table **4.1** is the entire conversion of linguistic crisp variables of multiple decision makers that volunteered for the survey. The corresponding fuzzy numbers and reciprocal values from Table **4.1** are indicated in Table **4.2**.

**Table 4.2: Fuzzy Triangular Fuzzy Numbers and Reciprocals Table**

|  |  |
| --- | --- |
| Fuzzy Numbers | Reciprocal |
| [1,1,1] | [1,1,1] |
| [0.5, 0.75, 1] | [1, 1.33, 2] |
| [0.67,1,1.50] | [0.67,1,1.50] |
| [1,1.50,2] | [0.50,0.67,1] |
| [1.50,2,2.50] | [0.40,0.50,0.67] |
| [2,2.50,3] | [0.33,0.40,0.50] |
| [2.50,3,3.50] | [0.29,0.33,0.40] |
| [3,3.50,4] | [0.25,0.29,0.33] |
| [3.50,4,4.50] | [0.22,0.25,0.29] |

The corresponding weights of fuzzy numbers and their reciprocal are used to compute the weights are computed using the fuzzy geometric mean given by Equation **3.2** as shown in Table **4.3**.

**Table 4.3: Weights of Learner Profile Information Attributes (Ww)**

|  |  |
| --- | --- |
| Attribute/Criteria | Weights  |
| Full Name | 0.0997 |
| Mobile Number | 0.1421 |
| Date of Birth | 0.1464 |
| Genotype | 0.0692 |
| Contact Address | 0.0524 |
| Medical Records | 0.0333 |
| CGPA | 0.1710 |
| Matric / Reg Number | 0.0055 |
| Marital Status | 0.1969 |
| IP Address | 0.0836 |

In Table **4.2**, the normalized weights are given by Equation **3.6** which converts the geometric mean weights to sum to **1**.Therefore, upon further processing, the percentage of influences, and sensitivity of attributes/criteria (rank) for privacy preservations as shown in Table **4.4**.

**Table 4.4: Normalized Weights (Wn) and ASI computation**

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute/Criterium | Weights  | Percent | Sensitivity |
| Full Name | 0.0997 | 9.97 | 5 |
| Mobile Number | 0.1421 | 14.21 | 4 |
| Date of Birth | 0.1464 | 14.64 | 3 |
| Genotype | 0.0692 | 6.92 | 7 |
| Contact Address | 0.0524 | 5.24 | 8 |
| Medical Records | 0.0333 | 3.33 | 9 |
| CGPA | 0.1710 | 17.1 | 2 |
| Matric / Reg Number | 0.0055 | 0.55 | 10 |
| Marital Status | 0.1969 | 19.69 | 1 |
| IP Address | 0.0836 | 8.36 | 6 |

From the Table **4.4**, the percentage of influences and sensitivity of attributes/criteria considered and decided by multi-decision makers. Accordingly, the most sensitive attribute is marital status (**19**.**69**%), followed by CGPA (**17**.**10**%), then, date of birth (**14**.**64**%). While, the least sensitive attribute is Matric/Reg.

Number. These are consistent with findings in (Mohanrao and Karthik, 2019; Atasoy et al., 2020; Turnbull, Chugh and Luck, 2021; Korac, Damjanovic and Simic, 2021). The charts of attributes selection based on sensitivity or weight value are shown in Figure **4.1**.

Figure **4.1**: Attributes Sensitivity Index of the Learner Profile Information.

Similarly, the fuzzy numbers plot for the developed Learner Profile Attributes Sensitivity Model using the fuzzy numbers and reciprocal numbers from Table **4.2** is shown in Figure **4.2**.



**Figure 4.2: Fuzzy numbers plot for LPAS model.**

# 5. Conclusion

In educational big data, privacy is contemplated due to the real danger of the Internet. The LMS harvest diverse digital identities about their learners, which are vulnerable to privacy compromises. Consequent upon this, this study proposed learner profile attributes partitioning model to determine sensitive and non-sensitive attributes in learners’ big data by means of FAHP. Then, privacy of these sensitive attributes is preserved from breaches during learning analytics operations of educators or education service providers.

The future studies could consider high-performance data features extraction and hiding techniques (such as blockchain) to disallow undue access or compromise of private learner information, learning content, and learning behaviors’

# 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>

Alharthi, A. D., Spichkova, M., & Hamilton, M. (2018). Sustainability requirements for eLearning systems: a systematic literature review and analysis. *Requirements Engineering*. <https://doi.org/10.1007/s00766-018-0299-9>

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>

Antonius, H., Widjaja, E., Santoso, S. W., Petrus, S., & Cahyadi, J. (2019). The Enhancement of Learning Management System in Teaching Learning Process with the UTAUT2 and Trust Model. *2019 International Conference on Information Management and Technology*, *1*, 309–313. IEEE.

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

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.

Chang, D.Y., 1996. Application of the extent analysis method on fuzzy AHP. Eur. J. Oper. Res. 95, 649–655.

Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2021). Enhancing the Usability of Cloud based LMS Architecture in Covid Pandemic. *Natural Volatiles & Essential Oils*, *8*(4), 7490–7511.

Chen, T., & Wu, H.-C. (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>

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](https://doi.org/10.1007/s40692-021%20-00218-4)

Ferguson, R. and Clow, D. (2017), “Learning analytics: avoiding failure, EDUCAUSE review”, available at: <https://er.educause.edu/articles/2017/7/learnin> g-analytics-avoiding-failure (accessed 15 May 2018)

Garone, A., Pynoo, B., Tondeur, J., Cocquyt, C., Vanslambrouck, S., Bruggeman, B., & Struyven, K. (2019). system. *British Journal of Educational Technology*, 1–18. <https://doi.org/10.1111/bjet.12867>

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.

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). <https://doi.org/10.1007/978-3-030-13743-4>

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.

Khan, H. U., & Alshare, K. A. (2019). Violators versus non-violators of information security measures in organizations — A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 4–23. <https://doi.org/10.1080/10919392.2019.1552743>

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>

Kumar, V., Kumar, D., Kumar, S., Bao, Q., Thi, N., Linh, T., … Tran, D. (2021). Development of fuzzy analytic hierarchy process based water quality model of Upper Ganga river basin , India. *Journal of Environmental Management*, *284*, 111985. <https://doi.org/10.1016/j.jenvman.2021.111985>

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>

Mohanrao, M., & Karthik, S. (2019). Privacy preserving for global data using approach. *Conference on Computer Vision and Machine Learning*, *1228*, 1–7. <https://doi.org/10.1088/17426596/1228/1/0120> 46

Muhammad, M. K., Oyefolahan, I. O., Olaniyi, O. M., & Adebayo, O. J. (2021). “An Intelligent Model for Detecting the Sensitivity Sentiments in Learners’ Profile on Learning Management System” *3rdSchool of Physical Sciences Biennial International Conference,* “The Role of Science and Technology in the Realisation of Research and Development in the Era of Global Pandemic” Federal University of Technology Minna, 25th  – 28th October, 2021. Pp 305 – 315.

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>

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>

Singh, H., & Miah, S. J. (2018). Design of a mobile-based learning management system for incorporating employment demands : Case context of an Australian University. *Education and Information Technologies*. [https://doi.org/https://doi.org/10.1007/s10639-018-9816-1](https://doi.org/https%3A//doi.org/10.1007/s10639-018-9816-1)

Turnbull, D., Chugh, R., & Luck, J., (2021). Issues in learning management systems implementation: A com- parison of research perspectives between Australia and China Education and Information Technologies <https://doi.org/10.1007/s10639-021-10431-4>, under exclusive license to Springer Science+Business Media, LLC part of Springer Nature 2021

Wang, Yaru, Zheng, N., Xu, M., Qiao, T., Zhang, Q., & Yan, F. (2019). Hierarchical Identifier: Application to UserPrivacy Eavesdropping on Mobile Payment App. *Sensors*, *19*(3052), 1– 19. <https://doi.org/10.3390/s19143052>.

Yee, J., Ooi, J., Kin, Y., & Andiappan, V. (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>