Information Security Assessment in Big Data Environment using Fuzzy Logic

Kanika Sharma, Achyut Shankar, Prabhishek Singh,
Sharma.kanika247@gmail.com, ashankar2711@gmail.com, psingh29@amity.edu,

Abstract- In recent years, it has been observed that disclosure of information leads to the risk. Without restrict the accessibility of information providing security is difficult. So, there is a demand of time to fill the gap between security and accessibility of information. In fact, security tools should be usable for improving the security as well as the accessibility of information. Though security and accessibility are not related directly, but some of their factors indirectly affect each other. Attributes play an important role in connecting the gap among security and accessibility. In this paper, finds the main attributes of security and accessibility that impact directly and indirectly each other such as confidentiality, integrity and availability and severity. The significance of every attribute in terms of their weight is important for their effect on the overall security during the big data security life cycle process. To calculate proposed work, researchers used the Fuzzy Analytic Hierarchy Process (Fuzzy AHP).

Keywords: Information Security, Big Data, Big Data Security Life Cycle, Fuzzy AHP

1. Introduction

Now a day's information and data are generated and handled at high velocity creating huge amounts of data. This huge amount of data is known as 'Big Data,'. Information and data is a tool that users used to transfer with them from that moment when they start to live together. Information technology's type and nature have been transformed radically in between previous years. This is the technical era, where information and data are created, managed, and processed at velocity developing a huge amount of data, information. This information generated from various sources such as social media, hospital database, bank transactions, etc. Thus, it's totally up to the users to consider the information is worthless or valuable [1]. The most common definition of information security is that information cannot be disclosed to anyone. It is a combination of three main components i.e. security, privacy, and accessibility [2].

Sharing information nowadays can pose jeopardy to any organization and user's privacy. Big data is a collection of a large amount of personal information that is easily accessible to be collected and analyzed. Organizations are a rich source of user's sensitive and personal information and epitomize supplementary opportunities for financially motivated cyber attackers [3]. Information security, privacy, and accessibility provide data security across the organization and are crucial in the complete operation of an organization. Together, they involve the users and techniques needed to reduce unauthorized access. Mohammadian et al. have suggested that sensitive and personal data can be classified with the help of fuzzy logic [4]. Hence, the main aim of organizations should be to prevent unauthorized access and provide security with accessibility.

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

So to accomplish this, various scientists are attempting to enhance the security by calculating it via various approaches. There is a lot of work available in this area but in literature, evaluating the attributes or security's characteristic and accessibility's characteristic by applicability on actual situations didn't meet. Moreover, the user is the whole sole

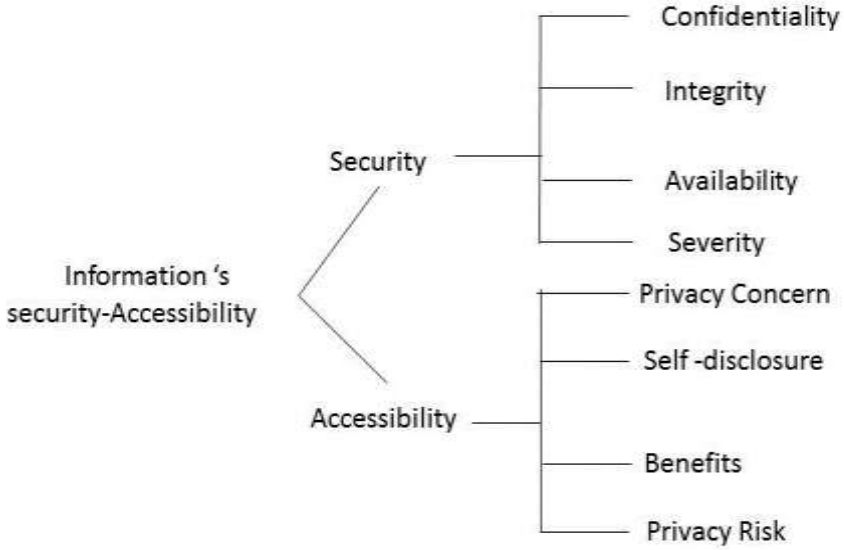

Figure 1: Hierarchy Structure of Attributes

individual who is responsible for his/her information security and its accessibility [[1]. Hence, provide security with accessibility to information is a crucial task but it's the demand for time in the big data environment is the demand. These paper goals are to secure the information with accessibility with MCDM methods by the combination of fuzzy [1].

So for this, the researchers classify the security's attributes (confidentiality, integrity, availability, and severity) as well as accessibility (privacy concerns, self-disclosure benefits, and privacy risk) attributes. Accessibility is the vital attribute to provide security at the time of disclosure of information. Hence, the people and originators need to understand the impact of both the attributes for fetching secure information. So the researchers are using the Fuzzy Analytic Hierarchy Process (Fuzzy-AHP) method for the assessment in this paper. For the evaluation, a hierarchy needs to establish which describes the affected attributes. With the help of the hierarchy and Fuzzy AHP method, security - accessibility of information has been calculated [2]. Outcomes obtained from the evaluation can support with the security of information at the time of the data generation/ creation phase in the big data life cycle [3]. The paper is organized as: II Section of this paper discusses the literature survey. In the Next section methodology has been discussed. Section IV provides an overview of the obtained results and finally, the conclusion in section V.

2. Literature Review

Security saving data mining was proposed in [5]. The study of the blend of cryptography strategies and security saving data mining techniques might be found in [6]. Different methods like randomization for grouping utilizing privacy-preservation have been examined. Cryptography based procedures [7] offer protection at a larger amount yet at the expense of

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020
DOI: 10.5281/zenodo.4099734

high calculation and correspondence required in such cases. The rundown of the association between the cryptography's fields and PPDM has been explained in [8]. In [9], displayed exhaustive and similar investigation of mystery sharing strategies for PPDM and Secure Multiparty Computation based systems and its proficiency. The authors proposed a preservation of privacy's estimation in data mining. The procedures of secure multiparty computation (SMC), homomorphic encryption (HE), and comparison has been helpful for techniques proposed in [10] [11].

A narrative risk evaluation methodology which includes 5sS metthod, FMEA, two fuzzy sets (IT2FSs), AHP and VIKOR was recommended for chemical laboratory in the work of Ozdemir et al. [12]. They included AHP and IT2FSs with FMEA's three parameters. Sutrisno et al. [13] used a practical approach of FMEA and modified it to use the complexity of the maintenance unused category. In a study, FMEA approach was modified Omidvar and Nirumand [14]. In this method VIKOR approach was used to identify and prioritize the modes of failure and apply fuzzy AHP technique to get the risk factors' weight in the operations in a study. Along with it the theories of Shannon entropy and Z number applied in this method too.
Zhang et al. have been underscores the detailed that in IS security human factors' importance has been identify by both researchers and organization, and conducted a studies survey on information security for user's awareness [31]. Y Chan et al. have developed a multifaceted method to encompass social and technical both the factors; still, past available literature on security behaviour with fuzzy of users have only dedicated on user's computer theft [30]. Azar and Darvishi have presented a model which shown the judgments of respondents' by defining the suitable functions of membership in a questionnaire with 5-point Likert scaled [28]. Carrasco et al. have been analysed the domains list with the help of fuzzy analysis [29]. Tuyls and Goseling have been showed in the research paper that with the helper data, the private removal can be possible from biometric data and extreme obtained private size is identical to the common information among the enrolled and queried structures. In this paper, they have been also verified that faultless security can be conceivable, if bits removed from the biometric structures and distributed uniformly [32]. In this paper, the researcher additionally offered a range for the helper information scheme is likely for privacy and personal disclose rate [33].

3. Methodology

3.1 Evaluation of Security- Privacy Attributes

The authors simultaneously consider risks and benefits in sharing personal information or reference information. Everything has two sides, so the technology offers easiness via social media and mobile phones on one side but on the second side, it has offered many issues related to privacy, security, data availability. Between all the problems discussed such as users' privacy and security are of paramount importance as users are disclosing their personal information on social media just for their enjoyment purpose [16]. Hence, when users expose or we can say they provide the accessibility of their personal information in social media, then they simultaneously consider privacy risk and benefits. A collection of reference information can disclose the patterns about the user's actual life. The context information that

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020
DOI: 10.5281/zenodo.4099734

has been disclosed on the internet can become a rich source to a hacker that means users is has been provided access to others [17].
Therefore, the researchers believe that this context information is a personal matter and when disclosing, users have to take privacy risks and benefits into consideration. There is a demand for time to evaluate security-accessibility for safeguarding the security of big data for ease of usage and satisfaction. The evaluation of the results of security -accessibility's attributes should be analyzed in-depth and can be used to improve the utility of security services. Priority analysis is performed by a Multi-Criteria Decision Making (MCDM) method [18]. This work donates as the security's prioritizing and privacy attributes through Fuzzy AHP with the inputs from experts. It detects ranks and weight of security- privacy's attributes. Figure 1 demonstrates security components i.e. confidentiality, integrity, accessibility, and severity, and privacy's attributes such as privacy concern, self-disclosure, benefits, and privacy risk which is more important than affecting the user's security. Security and privacy can be improved by focussing on its attributes together.

3.2 Fuzzy Set theory

A fuzzy set can be categorized via membership function. Fuzzy numbers are most commonly can be used in two ways, first is triangular numbers and second is trapezoidal fuzzy numbers. The researchers considered fuzzy numbers as triangular fuzzy numbers in this paper. Figure 2 represent a triangular fuzzy number, that is expressed as (f1,f2,f3) [15].

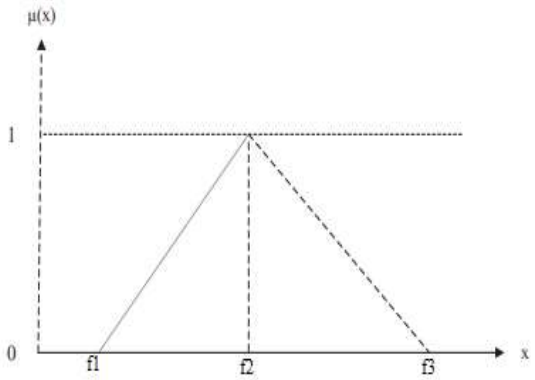

Figure 2: Triangular Fuzzy Number

$$\mu(x) = \begin{cases} \dfrac{x-f1}{f2-f1}, & \in [f1,f2] \\ \dfrac{f3-x}{f3-f2}, & x \in [f2,f3] \\ 0, & x < f1 \text{ and } x > f3 \end{cases} \quad (1)$$

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020
DOI: 10.5281/zenodo.4099734

$$\tilde{A} = \begin{array}{c} \\ F1 \\ F2 \\ \cdot \\ \cdot \\ Fn \end{array} \begin{array}{c} \begin{array}{cccc} F1 & F2 & \cdots & Fn \end{array} \\ \begin{bmatrix} 1 & a11\ldots\ldots & & a1n \\ 1/a2(1)1 & 1\ldots\ldots & & a2n \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 1/an1 & 1/an2\ldots\ldots & & 1 \end{bmatrix} \end{array} \quad (2)$$

several scholars have initiated that offers crisp numbers Fuzzy AHP is valuable by their weights, while AHP is considered worthy to examine a decision in a group [19, 20]. AHP is an essential apparatus that is often adopted by decision-makers. To handle the ambiguity and uncertainties of social decisions; the researchers have derived up with AHP's updated version which is called as Fuzzy AHP. Fuzzy AHP which is includes a fuzzy theory with the AHP approach [21]. Hence, the priorities of security-accessibility's attributes are essential to calculate the essentials attributes of these eight factors. Also, the contribution of every attribute in security-accessibility is calculated. So, in this section the prioritization of security-accessibility attributes to increase the security of information accessibility is discussed. The researchers have proved that for a small-scale MCDM problem, AHP is the best arrangement approach [21-23].

The main aim of the paper is to determine the priority of security- accessibility factors. For this, a questionnaire has been prepared. Thus, to answer the questionnaire it is necessary to have number of users who consider the information accessibility with its security. To evaluate the significance of security- accessibility factors, Fuzzy AHP is used because it can control fuzzy decision-related inputs given by participants [9,10]. For the better valuation of security accessibility in the form of rankings and weight then convert qualitative results into quantitative results [16, 27]. Additionally, the pairwise comparison matrix is arranged from the support of a questionnaire for the Fuzzy AHP approach. For calculating the weight of security-accessibility attributes, the applicant's inputs are converted into numeric values. The numeric values has been converted into Triangular Fuzzy Number (TFN) with the help of Equations (3)-(4) [24] and indicated as (Lo, Mo, Up), where Lo is lowest possible, Mo is most probable and Up is upper possible actions. Additional, Triangular Fuzzy Number is recognised as the following:

Let A1 = $(a_{ij})_{n\times n}$ and A2 = $(\alpha_{ij})_{n\times n}$ be two (TFN), where $a_{ij} = (Lo_1, Mi_1, Up_1)$ and $\alpha_{ij} = (Lo_1, Mi_1, Up_1)$. Now, tr(A1) = $\sum_{i=1}^{n} aij$ = (Lo, Mo, Up), where Lo = $\sum_{i=1}^{n} \alpha ij$, Mo= $\sum_{i=1}^{n} mij$ and Up = $\sum_{i=1}^{n} \alpha ij$. So

$$\tilde{A} \otimes \tilde{A} = (Lo_1, Mi_1, Up_1) \otimes (Lo_2, Mi_2, Up_2)$$
$$= (Lo_1 * Lo_2) , (Mi_1 * Mi_2), (Up_1 * Up_2) \ldots (3)$$

$$\hat{W} = \bar{r} \otimes (r_1' \oplus r_2' \oplus r_3' \oplus \ldots\ldots r_n) \ldots (4)$$

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

In the given equations, the values between two parameters the comparative significance, where i and j signify the pair of norms being determined by participants. The Value of a_{ij} is evaluated depends on the geometric mean for specific comparison. The geometric mean can correctly collect and representing the values [15] and signify the lower and upper scores correspondingly for the comparative position among the two criteria.

Centre of Area= (Lo+ Mo +Up)/3… (5)

A pair-wise comparison matrix of fuzzy is evaluated as n1 × n2 matrix, after calculating the values of TFN for every pairwise evaluation. Size of comparison matrix is 4 × 4, with a size of group limit to attain an adequate reliability's level.

Table 3: For Security's level 2 Pair-wise Comparison Matrix of Fuzzy.

	Confidentiality	Integrity	Accessibility	Severity
Confidentiality	1,1,1	0.433,0.614, 0.866	0.117, 0.197, 0.309	1.41, 0.107, 0.79
Integrity		1,1,1	0.080, 0.119, 0.184	0.32, 0.67, 0.84
Accessibility			1,1,1	0.047, 0.064, 0.118
Severity				1,1,1

Table 4: level 1's security and accessibility Pair-wise Comparison Matrix

	Security	Privacy	Weights
Security	1	0.877	0.725
Privacy	0.122	1	0.275

Table 5: level 2's security pair wise comparison Matrix of Fuzzy

	Confidentiality	Integrity	Availability	Severity	Weights
Confidentiality	1	0.433	0.614	0.866	0.528
Integrity	0.080	1	0.119	0.184	0.107
Availability	0.17	0.197	1	0.309	0.171
Severity	0.047	0.069	0.118	1	0.194

Table 6: level 2's Accessibility Pair-wise Comparison Matrix of Fuzzy

	Privacy Concern	Self-disclosure	Benefits	Privacy Risk	Weights
Privacy Concern	1	0.750	0.574	0.432	0.459
Self-disclosure	0.285	1	0.236	0.195	0.187
Benefits	0.132	0.126	1	0.112	0.097
Privacy Risk	0.063	0.179	0.741	1	0.257

Table 7: Results evaluation via Fuzzy AHP.

Attributes of 1st Level	Level 1's local weights	Attributes of 2nd Level	Level 2's Local Weights	Total Weights

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

S1	0.725	S11 S12 S13 S14	0.528 0.107 0.171 0.194	0.382 0.077 0.123 0.140
S2	0.275	S21 S22 S23 S24	0.459 0.187 0.097 0.257	0.126 0.014 0.026 0.066

Table 8: level 1's Security and Accessibility Pair-wise Comparison Matrix

	Security	Privacy	Weights
Security	1	0.352	0.529
Accessibility	0.106	1	0.471

Table 9: Aggregated Pair-wise Comparison Matrix for Accessibility at Level 2.

	Privacy Concern	Self-disclosure	Benefits	Privacy Risk	Weights
Privacy Concern	1	1.258	0.3876	0.4368	0.5576
Self-disclosure	0.1115	1	0.3876	0.3876	0.2516
Benefits	0.1840	0.0830	1	0.1292	0.1292
Privacy Risk	0.0780	0.0503	0.0503	1	0.0624

Table 10: Level 2's Security Pair-wise Comparison Matrix

	Confidentiality	Integrity	Availability	Severity	Weights
Confidentiality	1	0.650	0.8040	0.3595	0.5973
Integrity	0.1194	1	0.0663	0.2157	0.1300
Availability	0.1493	0.3900	1	0.1438	0.2010
Severity	0.0830	0.0429	0.1005	1	0.0719

In this evaluation, participants include online users such as academicians and students with both security-accessibility experiences. These candidates were selected to confirm the reliability of the AHP test. After calculation of qualitative, the pair-wise membership of TFN and decision matrix has been created after performed the function. In table 1, the participants' responses have been shown. The matrix arranged by the authors after evaluated the responses [25]. After qualitative calculation, in third step TFN function and pairwise comparisons matrix are evaluated to generate fuzzy's decision matrix which has been established. Additional, after create the comparison matrix; to generate measurable values which is depend on the TFN calculated values then defuzzification is performed. In this work, defuzzification approach has been adopted from [25] as formulated in Equation (5).

4. Result Evaluation

The values of CR (Consistency Ratio) are less than 0.1. CR values and the security-accessibility attributes independent weight are represented in Tables 4–6. Figure 3 represent the graphical representation of local weights of level 1. Figure 4 and figure 5 also represent

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

the weight level 2 and 3.Table 4 shows the local weight of the de-fuzzified level 1 and pair-wise comparison matrix characteristics. Through the results, its clear security is more important than accessibility to balance the accessibility of information. Table 5 represents the level 2 attributes for security independent weights and the defuzzified pair-wise comparison matrix. Table 7 represents the independent weights and attributes of level 2's defuzzified pair-wise comparison matrix for accessibility. Table 7 represents the overall ranking and dependent weights of the hierarchy.

Insecurity accessibility, security has 0.725, and accessibility has 0.275, means security is further essential than accessibility and needed a stability among accessibility and

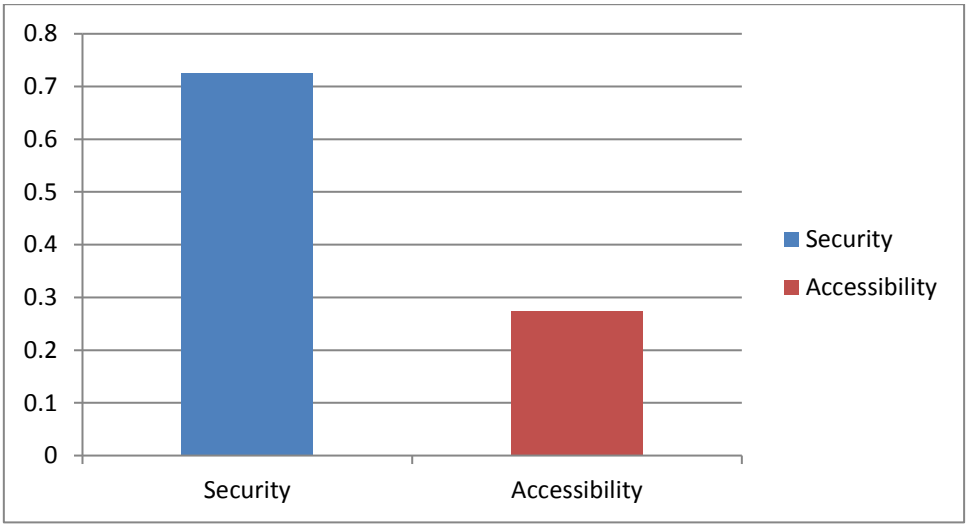

Figure 3: local's weight of Level 1

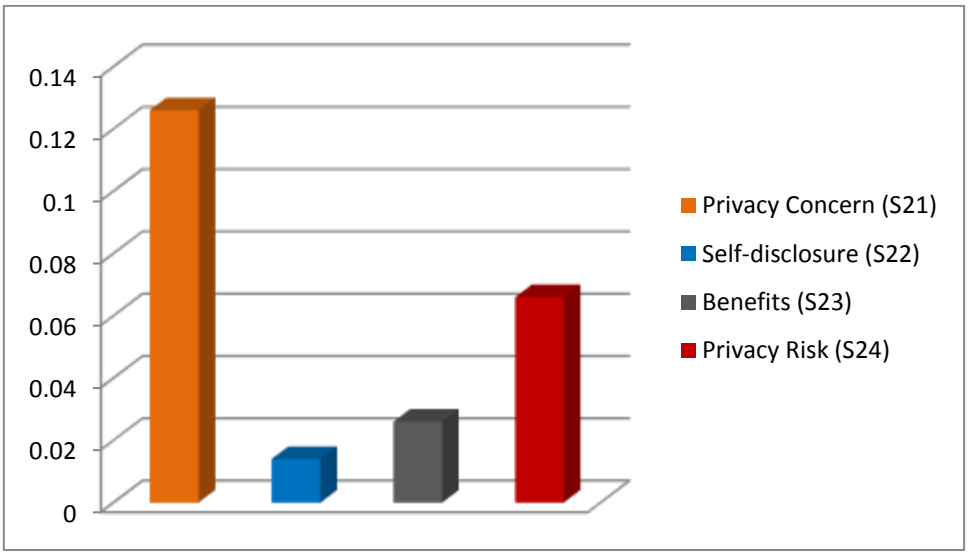

Figure 4: level 2's local weights

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

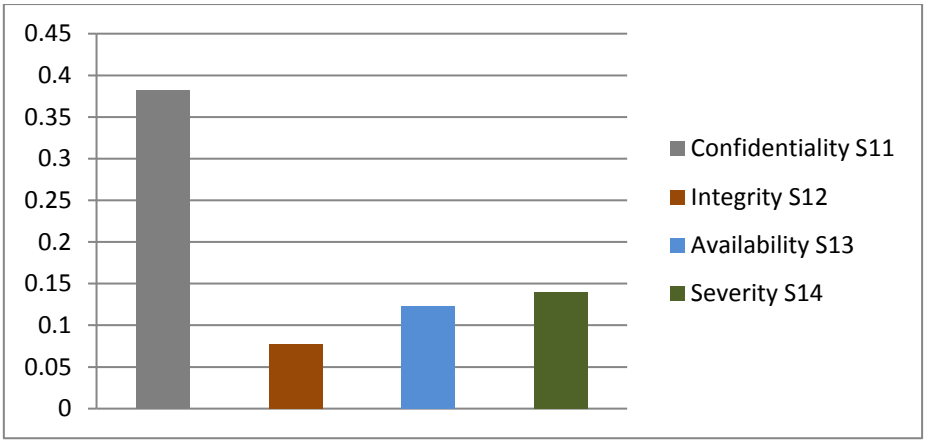

Figure 5: local weights of level 3

Table 11: Results Evaluation via AHP.

Level 1 Attributes	Level 1 Local Weights	Level 2 Attributes	Level 2 Local Weights	Total Weights
S1	0.529	S11 S12 S13 S14	0.5973 0.1300 0.2010 0.0719	0.315 0.069 0.107 0.038
S2	0.471	S21 S22 S23 S24	0.5760 0.2516 0.1292 0.0624	0.272 0.119 0.061 0.030

Table 12: Comparison between the Fuzzy- AHP and AHP Results

S.no	**Security and Accessibility Attributes**	**Fuzzy-AHP**	**AHP**
1.	Confidentiality	0.382	0.315
2	Integrity	0.077	0.069
3.	Accessibility	0.123	0.107
4.	Severity	0.140	0.038
5.	Privacy Concern	0.126	0.272
6.	Self-disclosure	0.014	0.119
7.	Benefits	0.026	0.061
8.	Privacy Risk	0.066	0.030

security. After implementing through Fuzzy AHP approach, another method has been also used known as the AHP method to prove the complete accuracy of result and estimation. To prove the results accuracy, the Security and accessibility's effect of various types evaluated from AHP. Data collection's process in classical AHP and but there is only one difference in

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

classical AHP is that no de-fuzzification is needed. So, for classical AHP, the data is comes in the form of crisp [26]. Figure 6 depicts the graphical representation on results.
A decision hierarchy is developed in the traditional AHP. Next, pairwise matrix of participants' opinions has been established but in this technique, numeric values used directly rather than TFN values. Another phase is to combine the comparison matrix's pairwise of participants' opinions while checking CR. Table 8 shows the level 1's independent weights and the combined comparison matrix's of pairwise. So it is obvious from result that security is essential in comparison rather than accessibility to improve the complete security. Table 9 depicts the combined comparison matrix of pairwise and independent weights of the security attributes of level 2. Table 10 shows the level 2's local weights and combined comparison matrix pair-wise of security's factors. The dependent weights and the overall ranking of the hierarchy are shown in Table 11. In table 12, the comparison's results of security and accessibility evaluation via both the fuzzy AHP and traditional methods of AHP has been represented. It can be seen that while using the Fuzzy-AHP, results are better and efficient in comparison to AHP. The difference among the results from both the methods Fuzzy AHP and AHP is shown in figure 6 and table 12.

5. Conclusion

Nowadays, security is one of the essential quality attributes for all users. The purpose of this paper is to evaluate the security accessibility of information at the data creation phase of big data security life cycle. The model proposed in this paper will help to calculate the security of information. The author has examined in this contribution, the author has examined eight security and accessibility factors throughout the big data life cycle. In this research, the attributes of security and accessibility are recognized. Users want to access information as well as the security of their personal data. But providing access to security is a tedious task. In this paper, the calculation of security-accessibility is a multi-purpose measures decision difficulty, Fuzzy AHP has been used to calculate the security accessibility. Most essential characteristics have also been calculated about weight. In the big data environment if we want to provide a secure environment to any user then we have to restrict the access of information. For the assurance of security accessibility, at the data creation phase, developers need
to restrict the access of information and focus on the information's security.

References

1. Sharma, K., Agrawal, A., Pandey, D., Khan, R. A., & Dinkar, S. K. (2019). RSA based encryption approach for preserving confidentiality of big data. Journal of King Saud University-Computer and Information Sciences.
2. Ak, M. F., & Gul, M. (2019). AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis. Complex & Intelligent Systems, 5(2), 113-126.

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

3. Kanika, A., & Khan, R. A. (2018). An Improved Security Threat Model for Big Data Life Cycle. Asian Journal of Computer Science and Technology, 7(1), 33-39.
4. Mohammadian, M., & Hatzinakos, D. (2017). A hierarchical fuzzy logic systems frame work for data security. International Journal of Information Technology, 9(2), 147-157.
5. R. Agrawal and R. Srikant, "Privacy Preserving Data Mining. ACM SIGMOD", Proceedings of International Conference on Management of Data, pp. 439-450, 2000.
6. B. Pinkas, "Cryptographic Techniques for PrivacyPreserving Data Mining", Available at: http://www.pinkas.net/PAPERS/sigkdd.pdf
7. S. Verykios et al., "State of the-Art in Privacy Preserving Data Mining", ACM SIGMOD Record, Vol. 33, No. 1, pp. 50-57, 2004.
8. J. Brickell and V. Shmatikov, "Privacy-Preserving Classifier Learning", Proceedings of 13th International Conference on Financial Cryptography and Data Security, pp. 1-6, 2009.
9. M. Upmanyu, A.M. Namboodiri, K. Srinathan and C.V. Jawahar, "Efficient Privacy Preserving K-Means Clustering", Proceedings of Pacific-Asia Workshop on Intelligence and Security Informatics, pp. 154-166, 2010.
10. G. Jagannathan and R.N. Wright, "Privacy-Preserving Distributed k-Means Clustering over Arbitrarily Partitioned Data", Proceedings of 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining, pp. 593-599, 2005.
11. P. Bunn and R. Ostrovsky, "Secure Two-Party K-Means Clustering", Proceedings of ACM International Conference on Computer and Communications Security, pp. 486-497, 2007.
12. Ozdemir, Y., Gul, M., & Celik, E. (2017). Assessment of occupational hazards and associated risks in fuzzy environment: A case study of a university chemical laboratory. Human and

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

Ecological Risk Assessment: An International Journal, 23(4), 895-924.

13. Sutrisno, A., Gunawan, I., & Tangkuman, S. (2015). Modified failure mode and effect analysis (FMEA) model for accessing the risk of maintenance waste. Procedia Manufacturing, 4, 23-29.
14. Mohsen, O., & Fereshteh, N. (2017). An extended VIKOR method based on entropy measure for the failure modes risk assessment–A case study of the geothermal power plant (GPP). Safety science, 92, 160-172.
15. Fattahi, R., & Khalilzadeh, M. (2018). Risk evaluation using a novel hybrid method based on FMEA, extended MULTIMOORA, and AHP methods under fuzzy environment. Safety science, 102, 290-300.
16. Jagwani, P., & Kaushik, S. (2017, March). Privacy in Location Based Services: Protection Strategies, Attack Models and Open Challenges. In International Conference on Information Science and Applications (pp. 12-21). Springer, Singapore.
17. Duckham, M., Kulik, L., 2005. A formal model of obfuscation and negotiation for location privacy.Pervasive Computing, 243–251.
18. Lin C, Jeng FL, Lee CS, Raghavan R (1997) Hierarchical fuzzy logic water-level control in advanced boiling water reactors. Nucl Technol 118:254–262.
19. IBM (2014) What is data security and privacy—overview. http:// www-01.ibm.com/software/data/security-privacy/. Accessed 13 June 2017.
20. Beckles, B., Welch, V., Basney, J., 2005. Mechanisms for increasing the usability of grid security. Int. J. Human Comput. Stud. 63 (12), 74–101. Buckley, J.J., 1985. Fuzzy hierarchical analysis. Fuzzy Sets Syst. 17.

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

21. Pérez-Domínguez, L., Rodríguez-Picón, L. A., Alvarado-Iniesta, A., Luviano Cruz, D., & Xu, Z. (2018). MOORA under Pythagorean fuzzy set for multiple criteria decision making. Complexity, 2018.
22. Deng, H. (1999). Multicriteria analysis with fuzzy pairwise comparison. International journal of approximate reasoning, 21(3), 215-231.
23. Ak, M. F., & Gul, M. (2019). AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis. Complex & Intelligent Systems, 5(2), 113-126.
24. Shyamal, A. K., & Pal, M. (2007). Triangular fuzzy matrices.
25. Voskoglou, M. (2015). Use of the triangular fuzzy numbers for student assessment. arXiv preprint arXiv:1507.03257.
26. Agrawal, A., Alenezi, M., Khan, S. A., Kumar, R., & Khan, R. A. (2019). Multi-level Fuzzy system for usable-security assessment. Journal of King Saud University-Computer and Information Sciences.
27. Dymova, L., Sevastjanov, P., & Tikhonenko, A. (2015). An interval type-2 fuzzy extension of the TOPSIS method using alpha cuts. *Knowledge-BasedSystems 83*, 116-127.
28. Azar, A., and Darvishi, Z. A., Development and validation of a measure of justice perception in the frame of fairness theory—fuzzy approach. Expert Syst. Appl. 38:7364–7372, 2011.
29. Carrasco, R. A., Muñoz-Leiva, F., Sánchez-Fernández, J., and Liébana-Cabanillas, F. J., A model for the integration of e-financial services questionnaires with SERVQUAL scales under fuzzy linguistic modeling. Expert Syst. Appl. 39:11535–11547, 2012.
30. Chan, M., Woon, I., and Kankanhalli, A., Perceptions of information security at the workplace: linking information security climate to compliant behavior. Journal of Information Privacy and Security 1(3):18–41, 2005.

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734

31. Zhang, J., Reithel, B. J., and Li, H., Impact of perceived technical protection on security behaviors. Information Management & Computer Security 17(4):330–340, 2009.
32. P. Tuyls and J. Goseling. Capacity and examples of template protecting biometric authentication systems. In LNCS, editor, Biometric authentication workshop (BioAW 2004), number 3087, pages 158–170, Prague, 2004.
33. T. Ignatenko. Secret-Key Rates and Privacy Leakage in Biometric Systems. PhD thesis, Eindhoven University of Technology, 200

Received: June 16, 2020 Revised: August 27, 2020 Accepted: October 9, 2020

DOI: 10.5281/zenodo.4099734