INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 2, PP. 245-250
Manuscript received May 6, 2021; revised May, 2022. DOI: 10.24425/ijet.2022.139874

Fuzzy Logic Based Intelligent Data Sensitive Security Model for Big Data in Healthcare

Somya Dubey, and Dhanraj Verma

***Abstract*—An intelligent security model for the big data environment is presented in this paper. The proposed security framework is data sensitive in nature and the level of security offered is defined on the basis of the data secrecy standard. The application area preferred in this work is the healthcare sector where the amount of data generated through the digitization and aggregation of medical equipment's readings and reports is huge. The handling and processing of this great amount of data has posed a serious challenge to the researchers. The analytical outcomes of the study of this data are further used for the advancement of the medical prognostics and diagnostics. Security and privacy of this data is also a very important aspect in healthcare sector and has been incorporated in the healthcare act of many countries. However, the security level implemented conventionally is of same level to the complete data which not a smart strategy considering the varying level of sensitivity of data. It is inefficient for the data of high sensitivity and redundant for the data of low sensitivity. An intelligent data sensitive security framework is therefore proposed in this paper which provides the security level best suited for the data of given sensitivity. Fuzzy logic decision making technique is used in this work to determine the security level for a respective sensitivity level. Various patient attributes are used to take the intelligent decision about the security level through fuzzy inference system. The effectiveness and the efficacy of the proposed work is verified through the experimental study.**

***Keywords*—microstrip patch; adaptive antennas; parabolic reflector; beamforming; antenna arrays; smart antenna**

I. Introduction

THE development in the field of healthcare sector has seen revolutionary over the last decade because of digitization of complete medical data referred as electronic medical records (EMR). It also has strengthened the research in terms of prognostic and diagnostic capabilities. EMR comprises of elementary information and medical history of the patients, clinical and doctor data, insurance information, etc. It also the readings and records generated through the internal and external sources like biometric data, genetics, blood pressure, electronic medical records, remote sensors data and social media data[1-3]. The processing of this huge amount of data requires large hardware with heavy cost and power.

Big data analytics has emerged as promising solution to deal with the huge amount of unstructured, semi-structured and structured data which cannot be processed by the conventional computing techniques. It is a distributed approach of processing the data even in the range of terabytes. The typical characteristics of big data are variety, volume, velocity and veracity which incorporate the size and heterogeneity of the data. The application of big data in healthcare sector can be proved useful in preventing epidemics, improving the quality of life, effectiveness of Clinical Trials, Detecting Side Effects of Drugs, etc. It can also avoid the preventable deaths through wise clinical decisions [4,5].

Considering the importance of the attributes of the patient's information in EMR, the security and privacy of the data has emerged as serious challenge. Any unauthorized access and unethical manipulation of the data may lead to large scale disaster medically and economically. The security of big data has been addressed by many researchers over the last decade and proposed different security models to prevent the data from the malicious attacks and leakages [6].

Three aspects of big data security for healthcare: data security, access control, and information security are discussed in [7]. They presented that the clinical and administrative information should be utilized for the security of the big data. The importance of data collection, storage, processing and analysis for the security is presented by [8] through the complete big data security cycle.

An authentication-based security model over Transport layer and secure socket layer for the communication of the data over the internet is also proposed in [9]. It works similar to the advance version of web technologies like web browsing, voice-over-IP (VoIP), electronic mail, Internet faxing, etc.

A novel one-time pad algorithm-based authentication model which discarded the need of passwords among the servers was proposed by [10]. They presented a security model where the customer's identity and the service provider's information must be verified at the time of access. Various encryption based security models like RSA, Rijndael, AES and RC6, DES, 3DES, RC4, IDEA, Blowfish, etc[11-16] have also been proposed to prevent the unauthorized access to the sensitive healthcare data throughout the security lifecycle. However, the variation of the size of the encryption key with respect to the data size poses a severe challenge to the researchers.

Data masking technology has also been used by some researchers to enhance the security of healthcare big data by replacing the sensitive data elements by unidentifiable values [17]. These data elements are then retrieved through a de-

Somya Dubey is with the Dr. A. P. J. Abdul Kalam University, Indore, India (e-mail: Somyadubey16@gmail.com).

Dhanraj Verma is with the Dr. A. P. J. Abdul Kalam University, Indore, India (e-mail: dhanrajmtech@gmail.com).

identifying strategy using quasi-identifiers. An approach based on k-anonymity of data masking for the healthcare big data to protect the identity is also proposed in [18]. This work is also extended by proposing p-sensitive anonymity by incorporating the attributes along with the identity parameters in the security framework [19]. However, these methods could not perform well over high dimensional dataset anonymity.

Access control-based security model has also been proposed by the researchers in the field of healthcare. Attribute based access control and cloud computing based dynamic access control strategy are proposed in [20,21] where they used a combination of cipher-text and encryption techniques.

Framework with big data analytics for healthcare sector are presented by [22] using various big data techniques. Huge amount of data is processed using the parallel architecture via hadoop, map reduce, pig Cassandra, Hbase, zookeeper, oozie, avro, mahout etc. The complexity of the algorithm has been optimized through parallel processing and distributed architecture.

However, the strategies proposed by the researchers for the security and privacy are static and uniform in nature. But the randomness and dynamism of the big data evolve a need of an adaptive and dynamic security model to deal with the uncertainty of the characteristics of the data. Adaptive security is the solution to this problem which offers a security technique based on examining the practices and occasions persistently and adjusts to the threats appropriately before they occur. Consistent observing and enhancements of security engineering are the fundamental needs of adaptive method. It anticipates to the unusual event, distinguish it and react before the attacker gets the opportunity to rupture the framework [23]. The major aspects of adaptive security are investigation and machine learning. The intelligent decision making about the unfamiliar event identification and offering the security is the core idea behind the adaptive security.

Over the last decade fuzzy logic has proved its potential in intelligent decision making in various applications. The capability of fuzzy logic control to map the complex mathematical framework into simpler linguistic architecture has really changed the paradigm of intelligent decision-making process. The computational complexity and the accuracy of the fuzzy logic-based control architecture is also superior than the conventional statistical techniques [24,25].

This paper presents an artificial intelligence based adaptive security model for the big data analytics for healthcare sector. The artificial intelligence in the proposed framework is implemented through the fuzzy logic decision making on the basis of the patient's and the best suited security model is provided in run time. The security model is data sensitive in nature which is determined by the parameters like patient information, medical history, insurance details, etc. The linguistic parameters are converted into fuzzy variables on the basis of their sensitivity level. Fuzzy inference system has been proposed in this work which takes the decision on the basis of these variables.

The major contribution of this work is the novel adaptive intelligent security framework using fuzzy logic. The security model is data sensitive and adaptive in nature which adds novelty to the research. It has combined the advantages of big data analytics to deal with the huge amount of data and the intelligence of fuzzy logic to make a decision in the presence of randomness, noise and uncertainties. This combined approach has added the robustness in the security model without compromising with the complexity level.

Remaining paper is organized as follows: section II deals with the preliminaries aspects of the Big data analytics and Healthcare sector. Fuzzy logic control is presented in section III. Section IV proposes the adaptive security framework implemented over the big data from healthcare. Performance of the proposed technique is evaluated in section V through the simulation study while section VII concludes the paper.

II. Big Data Analytics And Healthcare Sector

The amount of data which has been taken into consideration for the policy framework and market research by the organizations has changed the complete paradigm. The processing of this huge amount of data is defined as the big data analytics which extract the meaningful information from the data in a minimum possible time with high accuracy. The parallel processing frameworks of computing has been proved as a boon in big data analytics which has made it possible to identify the potential of the data for the decision making. The positive points of big data involve data mining, it is versatile and the mining is generalized. In Big Data, volume of data is generated with velocity and this volume of data contains varieties. Big data generates information on high dense data. It consists of unstructured and structured data, mostly the data it contains is unstructured and that is the biggest challenge. But the changes in last few years in IT automation sector are a big revolution. A big leap is taken in IT sector in different domains like Electronic Sector, Banking Sector, and E-commerce Sector.

Healthcare sector is also been changed a lot over the last two decades in terms of participation of technologies in the medical research and diagnosis. The available data of the medical records of millions of patients all over the world and their treatment history has changed the complete dynamics of the sector. This data has been used for the innovative treatment, focused care quality and value and evidence based medical practice instead of subjective treatment.

Big data analytics in healthcare sector has presented a great potential for completely changing the way of medical treatment and research. But it also has offered manifold challenges and constraints for the same. The biggest challenge associated with the implementation of big data over healthcare is the privacy and security of the EMR. The available security frameworks for the healthcare sector are not very efficient and secured for the ever-increasing threat of cybercrime. Any compromise with the medical record may be severely used by the malicious stakeholders and may results into a medical blunder all over the world. Therefore, security of the huge amount of medical data is a big concern for the researchers.

III. Fuzzy Logic Control

Fuzzy logic is decision making framework which is very close to the nature of human thought process. Unlike the crisp set decision making structure, fuzzy logic converts the linguistic

strategy into the overlapping decision sets. The selection of these sets is done on the basis of the human experiences which makes the decision realistic in practice. The implementation of fuzzy logic control is done through fuzzy inference system (FIS) which comprises of three stages: fuzzification, fuzzy inference logic and defuzzification. The complete process of fuzzy logic control is depicted in fig1. The first stage of fuzzification deals with the measurement of input variable and its mapping with the linguistics scale. Fuzzy inference logic stage is the real brain of the fuzzy logic control system. It includes the rule base which is responsible to take the decision. It defines the membership function for each parameter. The value of the membership function decides the outcome of the system. The whole intelligence of the fuzzy logic lies under the smartness of deriving these rule base and respective membership functions. Defuzzification stage coverts the linguistic variables again to the numerical values so as to generate the machine interfaced parameters.

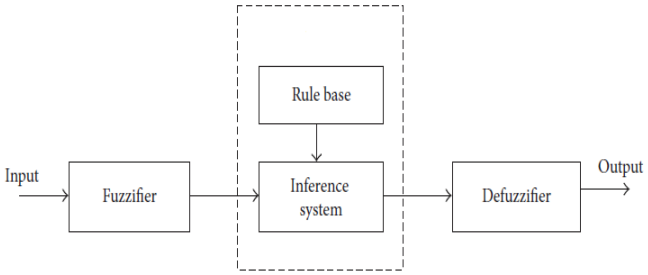

Fig 1. Fuzzy Logic system

IV. Fuzzy Logic Based Adaptive Security Model For Healthcare Big Data

The The proposed security framework for the healthcare big data encompasses three verticals of engineering: big data, Security and machine learning. It offers a data sensitive adaptive security model using the artificial intelligence. The intelligent classification and decision making is achieved through fuzzy inference system for the security model.

Security algorithms are the symmetric key cryptography and asymmetric key cryptography algorithms. It directly jumps on overhead and creates overhead in terms of memory and computation time because key is used in this algorithm and both sender and receiver hold their key to encrypt and decrypt data. Most of the popular and valued algorithms, which are used in existing research, called as BLOWFISH and RC6 algorithm, more different algorithms are as DES, AES etc. These algorithms work on key lengths from 32 bit to 1024 bit, 2048 bit, 2096 bit etc. with the increase in size, encryption time and decryption time increases. After data encryption, the cipher text we get is of large size.

The privacy and security of the EMR is of high importance in healthcare big data. The medical report, query file, patience name, surname, mobile number, city, country, e-mail address, investigation report in electronic health care system are of utmost value in medical research. But each attribute of a patient's data is not equally sensitive. For example, in case of a juvenile crime or crime against women like physical or sexual assault, the personal details of patient in the investigation report is very sensitive and can't be disclosed as per the legal constitutional obligations. But for other offences, these details may not be this much sensitive. Similarly, the medical reports of many patients contain different attributes of varying sensitivity. Applying the security of same level to all attributes is wastage of data rate and a compromise with throughput, latency, computation time, cost, processing duration, etc.

The solution to this problem has been proposed in this paper by offering different level of security to the data of different data sensitivity. Here, we import high level of encryption to the case with high sensitivity and lower security for the data of lower sensitivity like viral, having cold and cough, fever, etc. Various attributes of EMR are considered in this paper and they are been classified on the basis of the sensitivity level. Personal information, disease and the medical report are considered in this work. The sensitivity distribution assumed in this paper is shown in table 1.

Fuzzy inference system is derived in this paper to take decision on the level of security algorithm on the basis of the sensitivity level of these EMR attributes. Encryption is a well-established technique of providing secrecy and privacy to the data. Different encryption techniques have its speed and efficiency and ability to secure the protected data against attacks. The encryption techniques used in this work are discussed below in brief:

- Data Encryption Standard (DES): It is a simplest encryption technique proposed by National Institute of Standards and Technology (NIST) in 1974. It was later adopted for the military and non-military purpose by the US government. It uses a 64 bit key for a 64 bit plain text with 16 complex rounds and two transposition boxes. These16 rounds are iterated with same ciphers, but the first and last permutations are keyless straight permutations and an inverse of each other. The permutation takes a 64- bit key input and processes accordingly.
- Advanced Encryption Standard (AES): This encryption technique was developed by Vincent Rijmen, Joan Daeman in 2001 to overcome the limitations of DES. It is a symmetric encryption algorithm with three block ciphers namely AES- 128, AES-192 and AES-256. Each cipher text of 128- bits are processed using the keys of 128 bits, 192 bits and 256 bits respectively. The number of iterations for 128 bit key, 192 bit key and 256 bit key are 10, 12 and 14 respectively.
- Blowfish: It is an encryption technique proposed by a well known cryptologist, Bruce Schneir in 1993. This technique is simple and most commonly used encryption technique in public domain. It uses a 64 bit block cipher and variable length key. The implementation of this technique is comparatively more practical because of the optimal hardware design.
- RSA: RSA technique is named after the researchers, Rivest, Shamir and Adleman who invented it in year 1978. It is considered as a most secured way of encryption because of its popular exponentiation in a finite field over integers including prime numbers. It is an asymmetric cryptographic algorithm as it uses two different keys (public and private)

The security levels used in this paper corresponding to each data sensitivity level are DES, AES-128, AES-256, Blowfish, RSA for level 1 to level 5 respectively. The selection of the best suited encryption algorithm for the instantaneous data is derived

and decided by the proposed fuzzy inference systems. The overall working of the proposed security framework is shown in the form of a flow graph as shown in fig. 2.

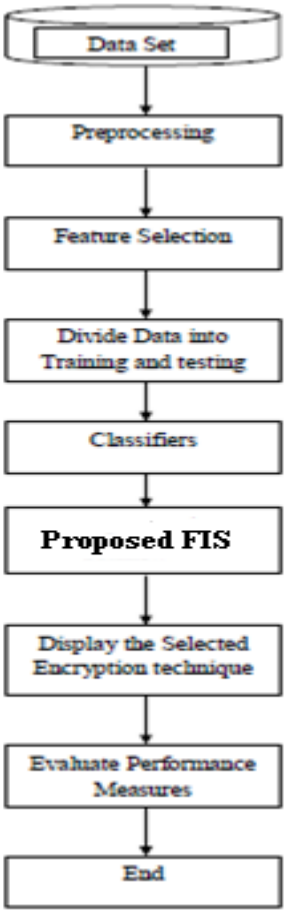

FIG. 2. Flow graph of the proposed security framework

TABLE I
SENSITIVITY DISTRIBUTION

Attributes	Classes	Sensitivity Level (Fuzzy Class)
Personal Information	Name	1 (Very Low)
	Age	2 (Low)
	Gender	3 (Medium)
	Mobile Number	4 (High)
	Address	5 (Very High)
Disease	Viral	1(Very Low)
	Different cases of cancer (on 1st stage)	2(Low)
	Sever Cancer	3(Medium)
	Infertility	4 (High)
	Rape victim level	5 (Very High)
Medical Report	Quantitative report (Pathological)	1(Low)
	Graphical reports like ECG, EEG, etc	2(Medium)
	Biomedical Images (MRI)	3(High)

V. RESULT ANALYSIS

The performance of the proposed adaptive security model is evaluated using the simulation analysis. Proposed work is verified on Electronic Health Care System where different size of data is used from 1MB to 5GB and then single cluster and multiple clusters are formed.

Requirements for Single cluster:

- I3 processor machine
- 4GB RAM
- UBUNTU 18
- HADOOP 2.7
- NetBeans

Using them a desktop application will be developed which is java based.

Requirements for Multi cluster:

- Heterogeneous system
- Using 4 machines, 1 cluster will be formed

The performance of the decision-making algorithm using the FIS is evaluated on the fuzzy rule set and the respective FIS. The proposed FIS is expected to generate the decision for the allotted encryption techniques for each data sample out of the following security techniques: DES, AES-128, AES-256, Blowfish, RSA for the data sensitivity of level 1 to level 5 respectively.

The input parameters for the fuzzy inference system considered in this work are the sensitivity level of personal information, disease and medical report. These parameters are converted into the linguistic version through the fuzzification process. The sensitivity level of Personal information and disease are fuzzified in 5 linguistic sets each viz, Very Low, Low, Medium, High and Very High. Medical report sensitivity is fuzzified as low, medium and high. Similarly, the out is derived in terms of R fuzzified as Very Low, Low, Medium, High and Very High mapped with the security level 1 to 5 respectively. The rule base is derived for the FIS system to take an efficient and accurate decision which is as shown in table 2.

TABLE II
FUZZY RULE-BASE

Rule No.	Sensitivity Level			Security Level
	Personal Information	*Disease*	*Medical Report*	
1.	Very Low, Low	Very Low, Low	Low	1
2.	Very Low	Very Low, Low	Medium	1
3.	Very Low	Very Low, Low	High	2
4.	Very Low	Medium	Low	2
5.	Very Low	Medium	Medium	3
6.	Very Low	Medium	High	4
7.	Very Low	High, Very High	Low	4
8.	Very Low	High, Very High	Medium	4
9.	Very Low	High, Very High	High	5
10.	Medium	Very Low	Low	2
11.	Medium	Very Low	Medium	2
12.	Medium	Very Low	High	3
13.	Medium	Medium	Low	3
14.	Medium	Medium	Medium	4
15.	Medium	Medium	High	4
16.	Medium	High, Very High	Low	4
17.	Medium	High, Very High	Medium	5
18.	Medium	High, Very High	High	5
19.	High, Very High	Very Low	Low	3

20.	High, Very High	Very Low	Medium	3
21.	High, Very High	Very Low, Low	High	4
22.	High, Very High	Medium	Low	4
23.	High, Very High	Medium	Medium	5
24.	High, Very High	Medium	High	5
25.	High, Very High	High, Very High	Low	4
26.	High, Very High	High, Very High	Medium	5
27.	High, Very High	High, Very High	High	5
28.	Medium	Very Low	Medium	2
29.	Medium	Very Low	High	3
30.	Medium	Medium	Low	3
31.	Medium	Medium	Medium	4
32.	Medium	Medium	High	4
33.	Medium	High, Very High	Low	4
34.	Medium	High, Very High	Medium	5
35.	Medium	High, Very High	High	5

The membership function type used in this fuzzy inference system is Gaussian. The respective FIS is as shown in fig.3.

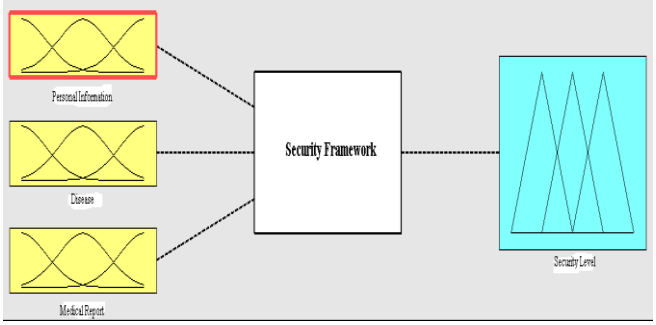

FIG 3. Proposed Fuzzy Inference System

The decision-making efficiency of the proposed framework is shown in fig.4. The 5 classes represent five encryption techniques corresponds to every medical data packet.

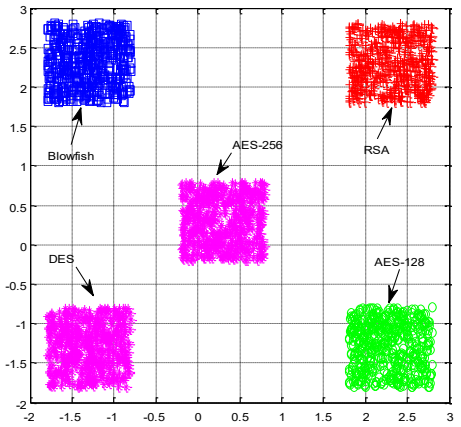

FIG 4. Fuzzy Logic based Security level Allotment

VI. CONCLUSION

An adaptive intelligent security framework is proposed in this paper which uses fuzzy logic for the data sensitive security. The proposed model is used for the security of healthcare dataset comprising of the patient details, disease attributes, medical reports as EMR. The features of the healthcare data is classified in the data sensitivity level as per the fuzzy logic and 5 different encryption techniques are used in this work as target security model which should be implemented depending on the sensitivity. The allocation of the best suited encryption technique for respective medical data packet is done by the FIS as per the rule base. The performance evaluation is performed for the security framework allotment and the accuracy attained through the simulation analysis reflects the effectiveness of the proposed technique. Offering low dimensional security to the data of low sensitivity reduces the algorithmic complexity and thereby enhances the throughput of the system. Also, the implementation of highest security method for highest sensitive data enhances the security level of the system.

REFERENCES

[1] S. Sharathkumar and G. Jagadamba, “Adaptive content-aware access control of EPR resource in a healthcare system,” 2017 International Conference on Advances in Computing, *Communications and Informatics (ICACCI)*, Udupi, 2017, pp. 205-210. http://dx.doi.org/10.1109/ICACCI.2017.8125841

[2] M. Jayabalan and T. O'Daniel, “Continuous and transparent access control framework for electronic health records: A preliminary study,” 2017 2nd International conferences on Information Technology, *Information Systems and Electrical Engineering (ICITISEE)*, Yogyakarta, 2017, pp. 165-170. http://dx.doi.org/10.1109/ICITISEE.2017.8285487

[3] R. Sánchez-Guerrero, F. A. Mendoza, D. Díaz-Sánchez, P. A. Cabarcos and A. M. López, “Collaborative eHealth Meets Security: Privacy-Enhancing Patient Profile Management,” in *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 6, pp. 1741-1749, Nov. 2017. http://dx.doi.org/10.1109/JBHI.2017.2655419

[4] A. Dev Mishra and Y. Beer Singh, “Big data analytics for security and privacy challenges,” 2016 International Conference on Computing, *Communication and Automation (ICCCA)*, Noida, 2016, pp. 50-53. https://doi.org/10.1109/CCAA.2016.7813688

[5] Beyer, Mark “Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data,” Archived from the original on July 2011. Retrieved 13 July 2011

[6] “Large-Scale Adaptive Machine Learning for Security Analytics, Ling Huang,” Joint work with ISTC and McAfee Labs ISTC Summer Retreat, OS/3112013.

[7] Kim S-H, Kim N-U, Chung T-M., “Attribute relationship evaluation methodology for big data security,” In: *2013 International Conference on IT convergence and security (ICITCS),* IEEE. p. 1–4, 2013. https://doi.org/10.1109/ICITCS.2013.6717808

[8] “Data-driven healthcare organizations use big data analytics for big gains,” IBM white paper February. 2013.3

[9] A. Yazan, W. Yong, N. Raj Kumar, “Big data life cycle: threats and security model,” In *21st Americas conference on information systems*, 2015.

[10] R. Zhang, L. Liu, “Security models and requirements for healthcare application clouds,” In: IEEE 3rd international conference on cloud computing. 2010. https://doi.org/10.1109/CLOUD.2010.62

[11] Xindong WU, Gong Qing WU and Wei Ding, “Data Mining with Big Data,” IEEE Transaction on Knowledge and Data Engineering, vol. 26, no. 1, pp. 97- 107, Dec. 2012. https://doi.org/10.1109/TKDE.2013.109

[12] G. Ghinita, “Privacy for location-based services synthesis,” Lectures on Information Security, Privacy, and Trust, University of Massachusetts, Boston, Tech. Rep., April 2013. https://doi.org/10.2200/S00485ED1V01Y201303SPT004

[13] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, “Pec: A privacy preserving emergency call scheme for mobile healthcare social networks,”

Communications and Networks, Journal of, vol. 13, no. 2, pp. 102–112, April 2011. http://dx.doi.org/10.1109/JCN.2011.6157409

[14] M. A. D. Mashima, D. Bauer and D. Blough, "User-centric identity management architecture using credential-holding identity agents," *Digital Identity and Access Management: Technologies and Frameworks, IGI Global*, December 2012. https://dx.doi.org/10.4018/978-1-61350-498-7.ch005

[15] F. Paci, R. Ferrini, A. Musci, K. Steuer, and E. Bertino, "An interoperable approach to multifactor identity verification," *IEEE Computer*, vol. 42, no. 5, pp. 50–57, 2009. http://dx.doi.org/10.1109/MC.2009.142

[16] R. Lu, X. Lin, and X. Shen, "Spoc: A secure and privacy preserving opportunistic computing framework for mobile-healthcare emergency," *Parallel and Distributed Systems, IEEE Transactions* on, vol. 24, no. 3, pp. 614–624, March 2013. http://dx.doi.org/10.1109/TPDS.2012.146

[17] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *Int J Uncertain Fuzziness Knowl Based Syst.* 2002;10:571–88. https://doi.org/10.1142/S021848850200165X

[18] P. Samrati, "Protecting respondents' identities in microdata release," *IEEE Trans Knowl Data Eng.* 2001;13:1010–27. https://doi.org/10.1109/69.971193

[19] TM Truta, B. Vinay, "Privacy protection: p-sensitive k-anonymity property," In: *Proceedings of 22nd international conference on data engineering workshops*. 2006. p. 94. https://doi.org/10.1109/ICDEW.2006.116

[20] A. Mohan, DM. Blough,"An attribute-based authorization policy framework with dynamic conflict resolution," In *Proceedings of the 9th symposium on identity and trust on the internet.* 2010. https://doi.org/10.1145/1750389.1750395

[21] H. Zhou, Q. Wen, "Data security accessing for HDFS based on attribute-group in cloud computing," In *International conference on logistics engineering, management and computer science (LEMCS 2014),* 2014. https://doi.org/10.2991/lemcs-14.2014.255

[22] H. Wang, J. Yin, C.S. Perng, & P. S. Yu, (2008, October), "Dual encryption for query integrity assurance," In *Proceedings of the 17th ACM conference on Information and knowledge management* (pp. 863-872). ACM. https://doi.org/10.1145/1458082.1458196

[23] J. Shafer, S. Rixner, Cox AL., "The hadoop distributed filesystem: balancing portability and performance," In *Proceedings of 2010 IEEE international symposium on performance analysis of systems & software (ISPASS)*, March 2010, White Plain, NY. p. 122–33. https://doi.org/10.1109/ISPASS.2010.5452045

[24] I. Tal, G.-M. Muntean, Towards Reasoning Vehicles:, "A Survey of Fuzzy Logic Based Solutions in Vehicular Networks," *ACM Comput. Surv*. 2018, 50, 80. http://dx.doi.org/10.1145/3125640

[25] P. Tillapart, T. Thumthawatworn, P. Viriyaphol, P. Santiprabhob, "Intelligent handover decision based on fuzzy logic for heterogeneous wireless networks," In Proceedings of the 2015 12th International Conference on Electrical Engineering/Electronics, *Computer, Telecommunications and Information Technology (ECTI-CON)*, Hua Hin, Thailand, 24–27 June 2015, pp. 1–6. https://doi.org/10.1109/ECTICon.2015.7207076

[26] C. Yang, W. Lin, M. Li, "A novel triple encryption scheme for hadoop-based cloud data security," In *Emerging intelligent data and web technologies (EIDWT)*, 2013 fourth international conference on. 2013. p. 437–42. https://doi.org/10.1109/EIDWT.2013.80

[27] Federal Information Processing Standards Publication 197. Specification for the advanced encryption standards (AES). 2001. https://doi.org/10.6028/NIST.FIPS.197