International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V70I8P103

Volume 70 Issue 8, 15-20, August 2022
© 2022 Seventh Sense Research Group®

Review Article

An Investigation Analysis on Secured Communication with Big Data

S. Sangeetha[1], P. Suresh Babu[2]

[1,2]*Department of Computer Science, Bharathidasan College of Arts and Science, Erode, India*

Received: 22 June 2022 Revised: 23 July 2022 Accepted: 02 August 2022 Published: 17 August 2022

Abstract *- Big data is a large volume of complex data structured and unstructured to reveal patterns and trends. Big data is a large amount of data storage and delivery on a semi-trusted big datasharing platform. Secured data communication is employed to perform the data point communication securely. Data security is an important role in guaranteeing a large number of data. Security in data communication transfers the message between sender and receiver to preserve the message as confidential. Cryptography performs the secured communication with an adversarial behaviour. Many researchers carried out their research for performing secured data communication. But, the data confidentiality level was not improved, and existing cryptographic methods did not reduce delay. Different cryptographic methods are discussed to perform the secured data communication to address these issues.*

Keywords *- Big data, Data confidentiality, Data delivery, Data storage, Cryptography.*

1. Introduction

Big data security protects against attacks, thefts and malicious activities. Big data security challenges are multi-faced for different companies. Big data was the new technology to present essential services for daily life. Big data sources vary from data sources in terms of quantity. Secure communications are an essential need in different applications. Secure transmission is described as the data transfer, like confidential information, through a secured channel. Secure communication is interacting with two entities and not allowing the third party to listen. The people shared the information with different degrees of certainty.

This paper is organized as follows: Section 2 reviews the efficient secured communication techniques with big data. Section 3 explains the existing secured communication methods. Section 4 discusses the experimental evaluation with possible comparisons. Section 5 describes the limitation of existing secured communication techniques. Section 6 concludes the paper.

2. Literature Review

A blockchain-based secure data sharing platform with fine-grained access control (BSDS-FA) was designed in [1] to address the privacy leakage issues during the data sharing process in the Internet of Things. But, the data confidentiality rate was not increased by BSDS-FA. A risk analysis approach is termed. Methodology for Analysis of Risks on Information System (MARISMA) was introduced in [2] for theBig Data environment. But, the execution time was not reduced by the risk analysis approach.

Blockchain-based identity authentication and trusted service evaluation were introduced in [3] to solve the unreliability issues for the submitted reviews. The users attained credible reviews of service vendors through the review publicity module. But, the security level was not reduced by blockchain-based identity authentication. Holistic Big Data Integrated Artificial Intelligent Modeling (HBDIAIM) was introduced in [4] to increase the privacy and security features of the data management interface in smart city applications. However, the data confidentiality rate was not increased by HBDIAIM.

Cybersecurity was provided in [5] for big data. The big data was protected for cybersecurity. But, the computational cost was not minimized by BDA. An anonymous and privacy-preserving federated learning scheme was designed in [6] for industrial applications. The federated learning scheme reduced privacy leakage through sharing parameters between the server and the participant. Though the accuracy level was increased, the security level was not increased.

A blockchain-based decentralized data trading system was introduced in [7] through smart contract-based data matching and reward allocation. But, time consumption for data communication was not minimized by the designed system. An efficient cloud storage system was introduced in [8] with the security restriction through the Hadoop framework on Apache Ambari. Ambari framework provided multi-layered protection for data stored in Hadoop distributed file system. But, the data confidentiality rate was not reduced by an efficient cloud storage system.

A new tensor-based optimization model was introduced in [9] for secure sustainable cyber- physical-social big data. The designed model optimized tasks in secure cyber-physical-social big data computation. But, computational complexity was not minimized by the designed model. PredictDeep framework was introduced in [10] for anomaly detection and prediction. The graph model gathered the analytical activities and interrelation. However, the data confidentiality was not increased by the PredictDeep framework.

Blockchain technology was introduced in [11] to handle the healthcare system by attaining better solutions. The designed scheme guaranteed better security with a smart contract. But, the delay time was not reduced by blockchain technology. A security scheme termed Lightweight Hybrid Scheme (LHS) was designed in [12] depending on Diffie-Hellman key exchange and Elliptic Curve Cryptography. But, the encryption time was not reduced by LHS.

3. Secured Big Data Communication

Big data is a new technology with many data with high velocity, high volume and high variety with management difficulty. Big data is the process of analyzing, storing and processing a large amount of data. Security in the era of big data and especially to the problem of reconciling security and privacy models by exploiting the map-reduce framework. Data can be classified as public, confidential and sensitive. Security was challenging in a big data environment with billions of devices and technologies for different security issues. The security mechanisms guaranteed the integrity and data suitability transmitted through communication devices and gateways. The data were transmitted to the destination node without tampering or distortion in the journey. A trust was carried out between communication devices where confidential data gets transmitted.

3.1. BDSS-FA: A Blockchain-Based Data Security Sharing Platform with Fine-Grained AccessControl

A blockchain-based secure data sharing platform with fine-grained access control (BSDS-FA) was introduced to address the privacy leakage issues during data sharing on the Internet of Things. A hierarchical attribute-based encryption algorithm employed the hierarchical attribute structure and multi-level authorization centre. The designed algorithm employed flexible and fine-grained access control by distributing user attributes to authorization centres. The designed algorithm combined with Fabric blockchain technology addresses the huge decryption cost issues for users with the Internet of things. Smart contracts in blockchain executed the high-complexity partial decryption algorithm to minimize the user decryption overhead. Blockchain recognized the traceability of historical operations to address the security needs of open and transparent supervision of data restriction. The designed hierarchical attribute-based encryption algorithm was considered CPA-safe. BDSS-FA provided secure and reliable data sharing services for users of the Internet of Things.

A hierarchical attribute-based encryption algorithm (HABE) was introduced to address data sharing access control issues. The system performance of a single authorization agency was increased by allocating different users to authorization centres for management. BSDS-FA presented the fine-grained access control for guaranteeing shared data security. Two smart contracts, namely validation contract and decryption contract, were designed depending on the fabric blockchain. The validation Contract was accountable for identifying the validity of user access rights. Decryption Contract was accountable for partial decryption of ciphertext in HABE. The decryption Contract minimized the computational overhead of the data consumer and increased the decryption performance.

3.2. MARISMA-BiDa pattern: Integrated risk analysis for big data

Data was essential for all companies, undoubtedly helping grow their quantity. Big Data appear in context as a collection of technologies that manage the data to attain the information for decision-making. Security risk in Big Data was examined appropriately to preserve the system and secure the information. A risk analysis approach termed Methodology for the Analysis of Risks on Information System (MARISMA) was introduced for Big Data environments. The designed approach depended on the security analysis method supported by many clients' technological environments in the cloud. MARISMA and eMARISMA were designed to get adapted for specific contexts like Big Data. MARISMA comprised two essential components, namely risk analysis and management process. The designed process was supported through an automated tool termed eMARISMA that helps in analysis and decision making. The designed process employed a particular pattern depending on the meta-pattern where MARISMA was applied to the IT environment. The two central components of the MARISMA methodology were reusable elements. MARISMA was adaptable and applicable to various contexts where patterns for different contexts were described with the elements of risk analysis and management process in meta-pattern.

3.3. BCSE: Blockchain-Based Trusted Service Evaluation Model over Big Data

A blockchain-based identity authentication scheme and trusted service evaluation model were introduced to address the unreliability issues submitted. The new trusted service evaluation model comprised blockchain-based identity authentication, evaluation submission, and evaluation publicity. In the evaluation model, authenticated users submit the reviews to the service vendors. The registration and authentication record of user identity and review for service vendors were stored in the blockchain network. The designed model guaranteed the credibility of user reviews for service vendors. The users obtain credible reviews of service vendors through the review publicity module.

A blockchain-based decentralized identity authentication scheme was designed with a trusted service evaluation model depending on the authentication scheme. An identity authentication function was employed through joining cryptography confidentiality and modification resistance of blockchain. Cryptography public keys and identity authentication records were accumulated in blockchain to form a continuous contextual data record structure. In the evaluation model, users who authenticate submit the reviews to the service provider. The identity authentication scheme minimized the dependence on the authentication centre and identified the identity authentication as transparent and auditable. The designed scheme increased the credibility of identity authentication. In the BlockChain-based trusted Service Evaluation (BCSE) model, users who passed authentication submit the reviews. User records of identity registration and authentication were stored in the blockchain to guarantee the evaluation authenticity obtained byservice vendors.

4. Performance Analysis of Secured Communication Techniques with BigData

To compare the secured communication methods, the number of data is considered input to the experiment. For experimental evaluation of three methods: blockchain-based secure data sharing platform with fine-grained access control (BSDS-FA), Methodology for Analysis of Risks on Information System (MARISMA) and Blockchain-based Identity Authentication, Mobile Health Human Behaviour Analysis is taken from Kaggle. HEALTH (Mobile HEALTH) dataset includes the body motion and vital signs recordings of ten volunteers with different profiles while performing various physical activities. Sensors placed on the subject's chest, right wrist and left ankle are used to determine the motion experienced by different body parts, namely, acceleration, rate of turn and magnetic field orientation. The sensor on the chest provides 2-lead ECG measurements for heart monitoring. Result analysis of existing techniques are determined with certain parameters are

- Data delivery ratio
- Data confidentiality rate and
- Processing time

4.1. Impact on Data Delivery Ratio

The data delivery ratio is the number of data correctly delivered to an authorized user. It is computed as

$$DDR = \frac{No.\ of\ data\ correctly\ delivered\ to\ an\ authorized\ user}{Total\ number\ of\ data} * 100 \quad (1)$$

From (1), the data delivery ratio (DDR) is calculated. It is computed in terms of percentage (%). The method is more efficient when the data delivery ratio is higher.

Table 1 explains the data delivery ratio to the number of data ranging from 10 to 100. Data delivery ratio comparison takes place on an existing blockchain-based secure data sharing platform with fine-grained access control (BSDS-FA), Methodology for Analysis of Risks on Information systems (MARISMA) and Blockchain-based Identity Authentication. The graphical representation of the data delivery ratio comparison is described in figure 1.

Table 1. Tabulation of Data Delivery Ratio

Number of Data (Number)	Data Delivery Ratio (%)		
	BSDS-FA	MARISMA	Blockchain-based Identity Authentication
10	85	81	78
20	88	83	80
30	90	85	82
40	92	88	83
50	91	87	81
60	94	89	84
70	96	91	86
80	93	88	84
90	91	86	82
100	92	89	85

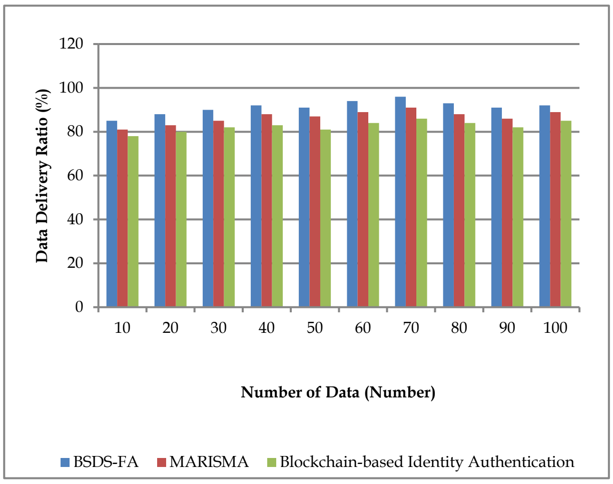

Fig. 1 Measurement of Data Delivery Ratio

From figure 1 above, the data delivery ratio depending on the different numbers of data is described. The blue colour bar denotes the data delivery ratio of BSDS-FA. The red and green bar correspondingly symbolizes the data delivery ratio of MARISMA and Blockchain-based Identity Authentication. The data delivery ratio using BSDS-FA is observed compared to MARISMA and Blockchain-based Identity Authentication. It is due to applying a hierarchical attribute-based encryption algorithm (HABE) for addressing access control problems in data sharing. The single authorisation agency's system performance was improved by allocating different usersto the authorization centres. This, in turn, helps to increase the data delivery ratio. The data delivery ratio of BSDS-FA is increased by 5% compared to the MARISMA and 11% compared to the Blockchain-based Identity Authentication.

4.2. Impact on Data Confidentiality Rate

Data confidentiality rate is the ratio of the number of data accessed by the authorized user to thetotal data. It is formulated as

$$DCT = \frac{Number\ of\ data\ accessed\ by\ authorized\ user}{Total\ number\ of\ data} \quad (2)$$

From (2), the data confidentiality rate (DCR) is computed. It is measured in terms of percentage (%). The method is more efficient when the data confidentiality rate is higher.

Table 2. Tabulation of Data Confidentiality Rate

Number of Data (Number)	Data Confidentiality Rate (%)		
	BSDS-FA	**MARISMA**	**Blockchain-based Identity Authentication**
10	78	89	84
20	81	90	86
30	83	92	88
40	85	94	90
50	82	91	89
60	80	89	86
70	78	87	83
80	80	88	85
90	82	90	87
100	84	94	90

Table 2 explains the data confidentiality rate to the number of data ranging from 10 to 100. Data confidentiality rate comparison takes place on an existing blockchain-based secure data sharing platform with fine-grained access control (BSDS-FA), Methodology for Analysis of Risks on Information systems (MARISMA) and Blockchain-based Identity Authentication. The graphical representation of the data confidentiality rate comparison is explained in figure 2.

In figure 2, the data confidentiality rate depending on the different numbers of data is explained. The blue colour bar denotes the data confidentiality rate of BSDS-FA. The red colour bar and green colour bars symbolize the data confidentiality rate of MARISMA and Blockchain-based Identity Authentication correspondingly. It is observed that the data confidentiality rate using MARISMA is higher when compared to BSDS-FA and Blockchain-based Identity Authentication. It is because of applying the security analysis method supported by the technological environment in the cloud for many clients. MARISMA and eMARISMA get adapted for Big Data during secured communication. This, in turn, helps to increase the data confidentiality rate. The data confidentiality rate of MARISMA is increased by 11% compared to the BSDS-FA and 4% compared to the Blockchain-based Identity Authentication.

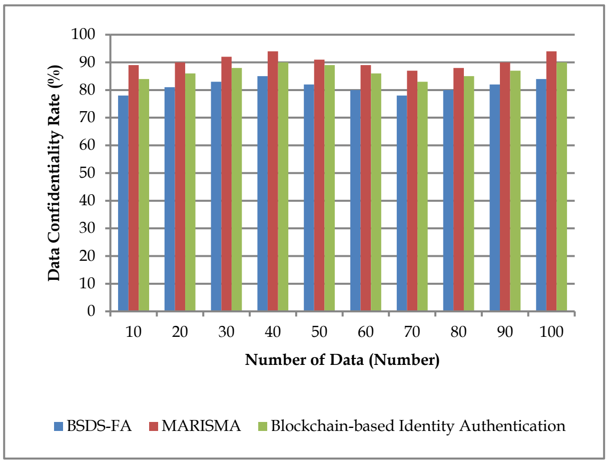

Fig. 2 Measurement of Data Confidentiality Rate

4.3. Impact on Processing Time

Processing time is defined as the amount of time consumed to perform secured data communication with big data. It is defined as the product of the number of data and the amount of time consumed by one data to perform secured communication. It is formulated as

$$PT = N * Time\ consumed\ to\ perform\ secured\ communication \quad (3)$$

From (3), the processing time (PT) is calculated. It is computed in terms of percentage (%). The method is more efficient when the data delivery ratio is higher.

Table 3. Tabulation of Processing Time

Number of Data (Number)	Processing Time (ms)		
	BSDS-FA	**MARISMA**	**Blockchain-based Identity Authentication**
10	35	40	22
20	37	42	25
30	40	45	27
40	42	48	30
50	44	51	32
60	46	53	34
70	48	56	37
80	50	58	39
90	52	60	41
100	55	62	44

Table 3 describes the processing time for the number of data ranging from 10 to 100. Processing time comparison takes place on an existing blockchain-based secure data sharing platform with fine-grained access control (BSDS-FA), Methodology for Analysis of Risks on Information systems (MARISMA) and Blockchain-based Identity Authentication. The graphical representation of the processing time comparison is described in figure 3.

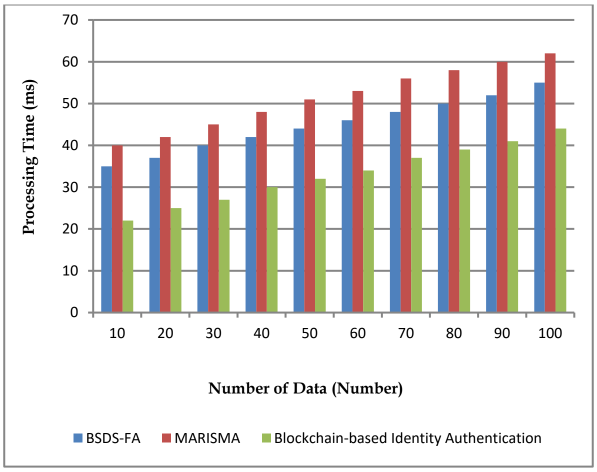

Fig. 3 Measurement of Processing Time

From figure 3 above, the processing time depending on the different numbers of data is explained. The blue colour bar denotes the processing time of BSDS-FA. The red colour bar and green colour bar represent the processing time of MARISMA and Blockchain-based Identity Authentication correspondingly. Processing time using Blockchain-based Identity Authentication is higher when compared to BSDS-FA and MARISMA. It is because of applying a blockchain-based decentralized identity authentication scheme with a trusted service evaluation model depending on the authentication scheme. An identity authentication function increases confidentiality with minimal time consumption. The processing time of Blockchain-based Identity Authentication is reduced by 27% compared to the BSDS-FA and 36% compared to the MARISMA.

5. Discussion and Limitation on Existing Secured Communication Methods with Big Data

BSDS-FA method was employed for addressing the privacy leakage issues through the data sharing process in the Internet of Things. The execution efficiency and user decryption performance were increased by the BSDS-FA method. A new hierarchical attribute-based encryption algorithm employed a hierarchical attribute structure and multi-level authorization centre. The algorithm performed the flexible and fine-grained access control by allocating different user attributes. But, the data confidentiality rate was not improved by the proposed BSDS-FA method.

A risk analysis approach termed Methodology for the Analysis of Risks on Information System (MARISMA) was introduced for Big Data environments. The designed approach depends on the security analysis method through the technological environment in the cloud using different clients. The risk analysis process was healthy and efficient for big Data. But, the execution time was not minimized by the risk analysis approach.

Blockchain-based identity authentication and trusted service evaluation were introduced to address the unreliability problems for submitted reviews. The users who were authenticated submit the reviews to service the vendors. The designed security model guaranteed the credibility of user reviews for service vendors. The users attained credible reviews of service vendors through the review publicity module. But, the security level was not reduced by blockchain-based identity authentication.

5.1. Future Direction

The future work direction can be carried out using deep learning techniques to increase secured data communication performance with a higher data delivery ratio and less time consumption.

6. Conclusion

A comparison of different existing secured data communication performances was described. From the study, it is observed that the security level was not reduced by blockchain-based identity authentication. The survival review shows that the risk analysis approach did not minimize the execution time. In addition, the data confidentiality rate was not improved by the proposed BSDS-FA method. The wide range of experiments on many secured data communication methods computes the performance with its limitations. Finally, the research can be carried out using machine learning and deep learning methods to increase the secured data communication performance.

References

[1] Hong Xu, Qian He, Xuecong Li, Bingcheng Jiang, and Kuangyu Qin, "Bdss-Fa: A Blockchain-Based Data Security Sharing Platform with Fine-Grained Access Control", *IEEE Access*, vol. 8, pp. 87552– 87561, 2020.

[2] David G. Rosado, Julio Moreno, Luis E. Sanchez, Antonio Santos-Olmo, Manuel A. Serrano and Eduardo Fernandez-Medina,“MARISMA-BiDa Pattern: Integrated Risk Analysis for Big Data”, *Computers & Security, Elsevier*, vol. 102, pp. 1-35, 2021.

[3] Fengyin Li, Xinying Yu, RuiGe, Yanli Wang, Yang Cui and Huiyu Zhou, "BCSE: Blockchain-Based Trusted Service Evaluation Modelover BigData", *BigData Miningand Analytics*, vol. 5, no. 1, pp. 1-14, 2022.

[4] Jie Chen L, Ramanathan and Mamoun Alazab, "Holistic, Big Data Integrated Artificial Intelligent Modeling to Improve Privacy and Security in Data Management of Smart Cities", *Microprocessors and Microsystems, Elsevier*, vol. 81, pp. 1-10, 2021.

[5] Danda B. Rawat, Ronald Doku and Moses Garuba, "Cyber Security in Big Data Era: From Securing Big Data to Data-Driven Security", *IEEE Transactionson Services Computing*, vol. 14, no. 6, pp. 2055–2072, 2021.

[6] Bin Zhao, Kai Fan, Kan Yang, Zilong Wang, Hui Li, and Yintang Yang, "Anonymous and Privacy-Preserving Federated Learning with Industrial Big Data", *IEEE Transactionson Industrial Informatics*, vol. 17, no. 9, pp. 6314– 6323, 2021.

[7] Donghui Hu, Yifan Li, Lixuan Pan, Meng Li and Shuli Zheng, "A Block Chain-Based Trading System for Big Data", *Computer Networks, Elsevier*, vol. 191, pp. 1-13, 2021.

[8] B. Mishachandar, S. Vairamuthu and M. Pavithra, "A Data Security and Integrity Framework using Third-Party Cloud Auditing", *International Journal of Information Technology*, Springer, vol. 13, pp. 2081–2089, 2021.

[9] Jun Feng, Laurence T. Yang, Ronghao Zhang, Shunli Zhang, Guohui Dai, and Weizhong Qiang, "A Tensor-Based Optimization Model for Secure Sustainable Cyber-Physical-Social Big Data Computations", *IEEE Transactionson Sustainable Computing,* vol. 5, no. 2, pp. 223-234, 2020.

[10] Marwa A. Elsayed and Mohammad Zulkernine, "Predict Deep: Security Analytics as a Service for Anomaly Detection and Prediction", *IEEE Access*, vol. 99, pp. 1-14, 2020.

[11] Pratima Sharma, Malaya Dutta Borah and Suyel Namasudra, "Improving Security of Medical Big Data by using Block Chain Technology", *Computers & Electrical Engineering, Elsevier*, vol. 96, pp. 1-15, 2021.

[12] Mallepalli Prasanna Kumari and Tumma Srinivasa Rao, "Alight Weighthy Brid Scheme for Security of Big Data", *Materials Today: Proceedings, Elsevier*, pp. 1-15, 2021.

[13] Maryann Thomas, S. V. Athawale, "Study of Cloud Computing Security Methods: Cryptography," *SSRG International Journal of Computer Science and Engineering,* vol. 6, no. 4, pp. 1-5, 2019. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V6I4P101

[14] Jun Feng, Laurence T. Yang, Ronghao Zhang, Shunli Zhang, Guohui Dai, and WeizhongQiang, "A Tensor-Based Optimization Model for Secure Sustainable Cyber-Physical-Social Big Data Computations", *IEEE Transactions on Sustainable Computing,* vol. 5, no. 2, pp. 223-234, 2020.

[15] WeichaoGao, Wei Yu, Fan Liang, William Grant Hatcher, Chao Lu, "Privacy-Preserving Auction for Big Data Trading Using Homomorphic Encryption", *IEEE Transactions on Network Science and Engineering,* vol. 7, no. 2, pp. 776-791, 2020.
DOI: 10.1109/TNSE.2018.2846736

[16] Saleh Atiewi, Amer Al-Rahayfeh, MuderAlmiani, Salman Yussof, Omar Alfandi, Ahed Abugabah, and Yaser Jararweh, "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography", *IEEE Access,* vol. 8, pp. 113498 – 113511, 2020. DOI: 10.1109/ACCESS.2020.3002815

[17] RafikHamza, Alzubair Hassan, Awad Ali, Mohammed Bakri Bashir, Samar M. Alqhtani, Tawfeeg Mohmmed Tawfeeg and AdilYousif, "Towards Secure Big Data Analysis via Fully Homomorphic Encryption Algorithms", *Entropy,* vol. 24, no. 4, pp. 1-17, 2022.

[18] Surabhi Singh, LataBajpai Singh, Anjali Rai, "Investigating the Analytics for Workforce Automation," SSRG *International Journal of Economics and Management Studies,* vol. 9, no. 5, pp. 23-31, 2022.
Crossref, https://doi.org/10.14445/23939125/IJEMS-V9I5P103

[19] Gayatri Kapil, Alka Agrawal, Abdulaziz Attaallah, Abdullah Algarni, Rajeev Kumar and Raees Ahmad Khan, "Attribute Based Honey Encryption Algorithm for Securing Big Data: Hadoop Distributed File System Perspective", *Peer J Computer Science,* vol. 6, 2020.

[20] Hanan E. Alhazmi, Fathy E. Eassa; Suhelah M. Sandokji, "Towards Big Data Security Framework by Leveraging Fragmentation and Block Chain Technology", *IEEE Access*, vol. 10, pp. 10768 – 10782, 2022. DOI: 10.1109/ACCESS.2022.3144632

[21] Akinsanmi Joel Akinboboye, Ayodele Sunday Oluwole, OlaitanAkinsanmi, Abiodun Ernest Amoran, "Cryptographic Algorithms for IoT Privacy: A Technical Review," *International Journal of Engineering Trends and Technology,* vol. 70, no. 8, pp. 185-193, 2022. *Crossref,* https://doi.org/10.14445/22315381/IJETT-V70I8P219

[22] SarathSabu, H.M. Ramalingam, M Vishaka, H.R. Swapna, SwarajHegde, "Implementation of a Secure and Privacy-Aware E-Health Record and IoT Data Sharing using Blockchain", *Global Transitions Proceedings, Elsevier,* vol. 2, no. 2, pp. 429-433, 2021.

[23] Shekha Chenthara, Khandakar Ahmed, Hua Wang, Frank Whittaker, Zhenxiang Chen, "Health Chain: A Novel Framework on Privacy Preservation of Electronic Health Records using Block Chain Technology", *PLoS ONE,* vol. 15, no. 12, pp. 1-35, 2020.

[24] Abhishek Gupta, Mahesh Pawar, Dr. SachinGoyal, RatishAgrawal, "Information Assurance via Big Data Security Analytics", *International Journal of Computer & organization Trends (IJCOT),* vol. 5, no. 2, pp. 85-91, 2015.

[25] JafarA.Alzubi, "Blockchain-Based Lamport Merkle Digital Signature: Authentication Tool in IoT Healthcare", *Computer Communications, Elsevier,* vol. 170, pp. 200-208, 2021.

[26] LokendraVishwakarma, Debasis Das, "SCAB-IoTA: Secure Communication and Authentication for IoT Applications using Block Chain", *Journal of Parallel and Distributed*.

[27] Shalini Kumari, Dr.Neeru Bhardwaj, "A Review Paper on Big Data," *SSRG International Journal of Mobile Computing and Application,* vol. 6, no. 2, pp. 1-3, 2019. *Crossref,* https://doi.org/10.14445/23939141/IJMCA-V6I2P101

[28] J. Hariharakrishnan, S. Mohanavalli, K. S. Kumar, et al., "Survey of Pre-Processing Techniques for Mining Big data," in *J Computer, Communication and Signal Processing (ICCCSP),* International Conference, pp. 1–5, 2017.

[29] W. Diffie, M. Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory,* vol. 22, no. 6, pp. 644-654, 1976.

[30] W. Stallings, "*Cryptography and Network Security: Principles and Practice*," 5th ed., Prentice Hall Press, Upper Saddle River, NJ, USA, 2010.

[31] P.Priya, R.Jayakumar, "Cryptography Based Privacy Preserving Data Transmission in Hybrid Wireless Networks", *International Journal of Computer & organization Trends (IJCOT),* vol. 6, no. 6, pp. 5-9, 2016.

[32] D. Mondek, R. B. Blazˇek, and T. Zahradnicky`, "Security Analytics in the Big Data Era," in *Software Quality, Reliability and Security Companion (QRS-C), IEEE International Conference,* pp. 605–606, 2017.