International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-10, Issue-02, May 2024

Health-HIDE: Design and Development of Hashing Identity based Data Encryption on Electronics Healthcare Records.

Swati Sanap, PG Scholar, ARMIET, Maharashtra, India, ssswatisanap15@gmail.com

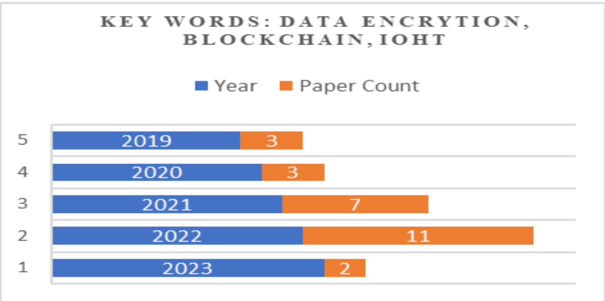
Vijay Shelake, Professor, University of Mumbai, Maharashtra, India, Vijaysnew12@gmail.com

Abstract: The days of maintaining paper records and relying mostly on fax machines for communication have long since passed in the healthcare sector. The paper chart of a patient is now digitally translated into Electronic Health Records (EHRs). The user could assume—to the dismay of the third party—that the original EHRs kept in the cloud have been altered when a medical disagreement arises. In addition, sharing data from cloud storage across many platforms with disparate access control settings is challenging. Drug development, disease prediction analysis, early warning epidemics, preventative healthcare, and patient health monitoring are just a few of the huge advantages that the Internet of Things (IoT) is offering to the healthcare industry. It also has the ability to completely transform the present healthcare system. Time-sensitive healthcare applications like ECG and EEG monitoring necessitate ongoing assessment of patient health data (PHD) and physician reports. In order to further our understanding of DM and to explore for a possible treatment, physicians and researchers also require data. Since obtaining such medical data is typically challenging for a variety of reasons (such as limited access to relevant data, pre-existing legal restrictions, and low user trust), it's critical to research novel approaches for large-scale automated data collecting. The IoMT is aided by fog computing, which also guards against data manipulation during information transfer across a secure network. Furthermore, the data is partially processed based on the demand. Subsequently, the gathered data is kept at the ledger unit via the blockchain network. Data encryption with hashing identity-based encryption is a type of public key encryption that protects sensitive information from prying eyes by encrypting it using a digital signature. At that point, the system performs at its peak in terms of responsiveness, time complexity, and actual user rate.

Keywords: ***IoHT, Fog Computing, EHR, Blockchain Technology.***

I. INTRODUCTION

This study used cybernetic patient health records, which are EHR-based records that include contact details, medical history, diagnosis, allergies, prescription medications, test results, and a comprehensive treatment plan. Cloud servers may reveal patient privacy when it comes to very sensitive and well-protected health data for profit. The existing medical system falls short in ensuring transparency, reliable traceability, immutability, audit, privacy, and security when maintaining electronic health records, and the loss of sensitive patient data has major repercussions. Through linked medical equipment, the Internet of Health Things (IoHT) is utilized to collect user data from sensors and send it to the cloud for storage.



II. LITERATURE REVIEW

Electronic Health Records (EHRs) are cybernetic versions of patient records that include personal contact details, medical history, diagnosis, allergies, prescribed drugs, test results, and a comprehensive treatment plan.

On account of this preventing EHR plays a major role in the medical department. This literature review explores the promise and challenges of existing research.

A tamper-proof blockchain authentication mechanism was presented by Norah et al. [1]; it has good capability, security, resilience to multiple assaults, and decreased latency. Furthermore, it offers group authentication that is both scalable and lightweight; on the other hand, the effectiveness of the suggested framework is directly correlated with the quantity of authorized devices. When used on a greater quantity of medical devices, group authentication exhibits increased efficiency. Nevertheless, there may be a drop in security if more medical devices are verified at the same time.

A three-tier blockchain technique based on FC and able to securely facilitate transactions and transmission close to the edge was developed by Saurabh et al. [2]. A mathematical

 DOI : 10.35291/2454-9150.2024.0135

framework and an FC-based blockchain analytical model for safe data transfer and transactions in the Internet of medical devices. Using a private blockchain, the architecture also handles the identification and verification of keys and certificates for fog nodes and IoT devices. On the other hand, extensive data transmission raises network traffic, which in turn raises data packet errors.

Abolfazl., *et al* [3] designed an Integrate IPFS and blockchain model to make the double-layer security. This leads to low latency and less energy consumption due to its inherent nature and efficiency in handling complex data with the capability of scalability. Although the implementation of the model for trauma services where real-time monitoring is critical. Naveed., *et al* [4] demonstrate Blockchain-based fog computing approach gives higher accuracy and is robust in terms of computational efficiency. This achieves the accuracy of different datasets in Hollywood2 - 87%, UCF50 - 90% and KTH - 75%.

Effective Blockchain-based safe healthcare services for illness prediction in fog computing are proposed by P.G. Shynu et al. [5]. Compared to previous approaches, our method predicts the illness and clusters efficiently. To improve the accuracy of the prediction findings, certain hybrid clustering and classification methods as well as security and privacy for patient medical data access can be incorporated.

Suparat., et al. [6] use scPBFT in a Consortium Blockchain to share electronic health data, enhancing the network's resilience and handling power. Additionally, it lessens the disruption caused by the Byzantine node and enhances the generation of the consensus outcome; nonetheless, in order to secure the patient's identity and electronic health record, homomorphic encryption and zero-knowledge proofing must be used.

A distributed ledger database is supported by a public-permissioned blockchain with an elliptic curve crypto digital signature created by Desire et al. [7]. This establishes and ensures the highest level of security for user data, resolves latency issues, and improves key generation times. Nevertheless, the application of a crypto hash cypher text, which will generate the PVT key, can secure and prevent the misuse of patient medical privacy data from being accessed by a compromised user.

A BIoT framework based on edge computing, BC, and IoT was developed by Sahar et al. [8]. It offers the healthcare industry a number of features, including the complete preservation of patient data, unaltered confidential transmission, and safe transmission of patient examination results. But this system has to be maintained and should be viewed as a cutting-edge telemedicine method that may help with a lot of problems. In order to increase security, the system can also include extra security-related technology.

Randhir, Kumar *et al.*,[9] are concerned a Consortium blockchain technology which provides efficient privacy and security for device-generated medical data, however, Less number of agents (peers) are used.

Although it is not yet widely utilised and there are just a few successful attempts, Neeraj Kumar et al. [10] presented a Dual-layer Blockchain-IoT used in the Swarm Exchange Paradigm to ease EHR data transmission by linking security services with HER blocks.

Israr Ahmad., *et al* [11] integrated and implemented IoT, fog, and blockchain-based systems in which the Fog storage reduces the latency. Then the critical messages are assigned as urgent alerts that call for immediate action in a condensed amount of time. Although the system receives more non-critical messages, the response time may increase.

A lightweight blockchain was created by Somchart Fugkeaw et al. [12] in order to achieve increased efficiency and reduced processing costs for both encryption and decryption. But since it doesn't address the visibility of characteristics within the ciphertext itself, this only partially resolves the problem.

An IoT CGM-based Blockchain technique was presented by Tiago M. et al. [13] and utilised to decentralise the database and assess smart contracts. However, by utilising quicker consensus techniques or other novel enhancements, the blockchain's reaction time may be accelerated.

In order to protect the confidentiality and integrity of patient data, Muhammad Umar Nasir et al. [14] created a Blockchain-based Edge computing and Fog computing approach. This makes it possible to analyse IoMT-generated data more quickly and reliably, but it also necessitates the implementation of new deep learning models that outperform the current models in terms of both computation and performance.

A FogChain was created by ANDRÉ. et al. [15] to enable the processing of IoMT-generated data more quickly and reliably. However, it ignores instances involving many nodes and operates on a single server executing containers.

In order to decrease communication time between IoMT devices, resource distribution, and network traffic congestion, Shadab Alam. et al. [16] use a Distributed BC cloud approach into their scheduling algorithms, even if these algorithms still need to achieve highly optimized energy efficiency and ultra-low latency.

Yanhui et al. [17] developed a distributed access control system based on blockchain that provides dynamic and fine-grained access control for Internet of Things data in order to overcome the problem of a single point of failure in access control. But to ensure the security and legality of edge nodes, computer technology is needed.

Marc Jayson Baucas [18] introduced a Private Blockchain with Fog-IoT, which effectively preserves a patient's

 DOI : 10.35291/2454-9150.2024.0135

International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-10, Issue-02, May 2024

privacy and a predictive service's integrity. However, need to improve the propagation delay between the fog and the cloud when transporting the training model.

Youyang Qu [19] developed a Blockchain-enabled Federated Learning that is used to poison attacks and could be eliminated from the aspect of fog server, but which had high computational cost, and insufficient efficiency.

In order to make bio-inspired sensors more reliable and secure, Abdullah et al. [20] created a Blockchain-fog-cloud-assisted IoMT technique; however, they did not take service mobility or fault tolerance into account.

Al and Humberto [21] A scalable method for a worldwide immunization with minimal latency—less than one second—was created by integrating blockchain technology with fog, but with fewer peers.

Muhammad Wazid and others [22] The fog computing-based healthcare system's AI-enabled secure communication mechanism (AISCM-FH) has been presented. It offers enhanced security, reduced communication and processing costs, and more functionality But there is less data carried by the system.

Insufficient efficiency is provided by the LoRaChain-Care that Bouthaina et al. [23] designed for the safe and authorised sharing of health data, including patient vital signs and medical reports.

A MediBchain concept was incorporated by Abdullah Al Omar et al. [24]. It is inexpensive, offers effective privacy and security, but requires interoperability across many institutions.

A technology called Fortified-Chain was created by Bhaskara S et al. [25] and yields minimal latency, low traceability, high data security, and privacy. But a strong system must improve the calibre of the services.

III. PROPOSEDED METHODOLOGY

In this Research article which is used to transfer the data without any losses and prevent data from adversaries. Internet of Health Things (IoHT) is leveraged by IoT, which will capture user data from sensors and transfer data to the cloud for storage through connected medical devices. and also, the IoMT devices are used to monitor and classify the users and intruders. The multimodal biometric-based authentication scheme will be used to provide potential security to the IoMT sensors and fog chain by using a person's biological features. Fog computing is used to promote the IoMT and prevent data tampering at the transmission of information in a secure network. In addition, depending on the requirement which is partially processed the data. Then the collected information is stored at the ledger unit through the blockchain network. The blockchain network will be used to secure the data from third parties, if any data should be read/stored in the ledger the blockchain network sends a request to the ledger. The ledger checks the request and confirms which is correct to allow access to the data. Hashing identity-based data encryption is a public key encryption, which uses a digital signature to encrypt the data to prevent the data from a third party. The evaluation will be done based on the performance metrics that is time complexity.

IV. RESULT AND DISCUSSION

In the result and discussion of this research article to analyze and evaluate the performance of based on the time complexity.

Data Encryption Time on Dataset 1:

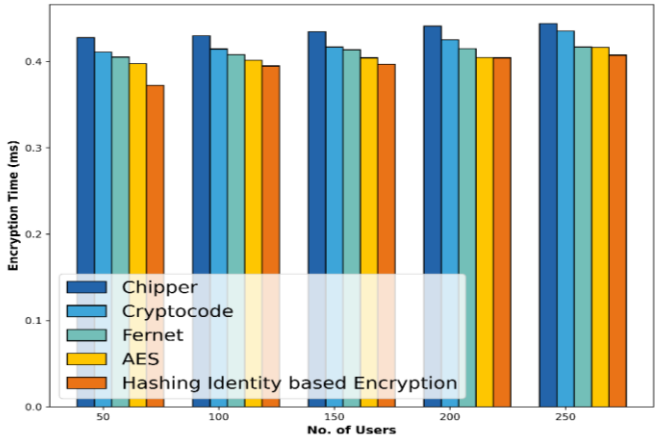


Fig 1: Encryption Time on Dataset 1.

Decryption Time on Dataset 1:

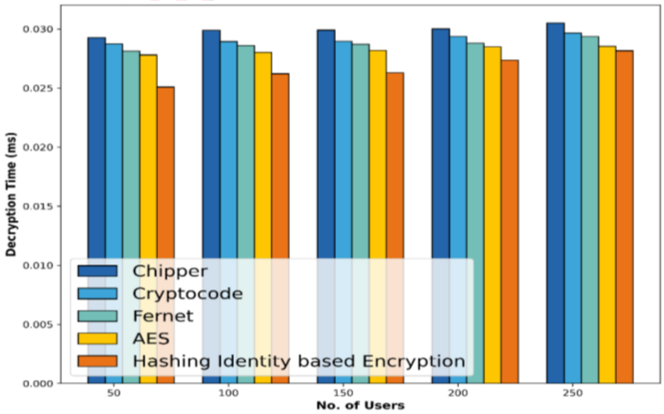


Fig: Decryption Time on Dataset 1.

Model	50 Users	100 Users	150 Users	200 Users	250 Users
Chipper	0.427	0.429	0.434	0.440	0.443
Cryptocode	0.410	0.414	0.416	0.425	0.435
Fernet	0.405	0.408	0.413	0.414	0.416
AES	0.397	0.401	0.404	0.404	0.416
Hashing Identity - Encryption	0.372	0.394	0.396	0.404	0.407

Tbl 1: Data Encryption Time

Model	50 Users	100 Users	150 Users	200 Users	250 Users
Chipper	0.029	0.029	0.029	0.030	0.030
Cryptocode	0.028	0.028	0.028	0.029	0.029

 DOI : 10.35291/2454-9150.2024.0135

ISSN : 2454-9150 Vol-10, Issue-02, May 2024

Fernet	0.028	0.028	0.028	0.028	0.029
AES	0.027	0.028	0.028	0.028	0.028
Hashing Identity - Encryption	0.025	0.026	0.026	0.027	0.0281

Tbl 2: Data Decryption Time

CONCLUSION

The demand of novel healthcare system provides security of stored health data during transfer. The multimodal biometric-based authentication scheme and hashing identity-based data encryption layers are used to provide high security. The responsiveness of the proposed system will be aimed better than the exited system, which is greater than 100 transactions per second. The time complexity and Genuine user rate of the proposed system will be improved than the previous systems. In the performance analysis time complexity where encryption time model that are chipper, Cryptocode, fernet, AES, and hashing identity-based encryption to reduce the losses that is 0.44, 0.43, 0.4167, 0.4161 and 0.407% on the basis of the 250 users.

ACKNOWLEDGMENT

My research supervisor and the faculty have provided me with ongoing support and direction, for which I am incredibly grateful. I also want to express my gratitude to everyone that helped me out with my study, both directly and indirectly.

REFERENCES

[1] Alsaeed, Norah, Farrukh Nadeem, and Faisal Albalwy. "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing." Future Generation Computer Systems 151 (2024): 162-181.

[2 Shukla, Saurabh, Subhasis Thakur, Shahid Hussain, John G. Breslin, and Syed Muslim Jameel. "Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model." Internet of Things 15 (2021): 100422.

[3] Mehbodniya, Abolfazl, Rahul Neware, Sonali Vyas, M. Ranjith Kumar, Peter Ngulube, and Samrat Ray. "Blockchain and IPFS integrated framework in bilevel fog-cloud network for security and privacy of IoMT devices." Computational and Mathematical Methods in Medicine 2021 (2021).

[4] Islam, Naveed, Yasir Faheem, Ikram Ud Din, Muhammad Talha, Mohsen Guizani, and Mudassir Khalil. "A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services." Future Generation Computer Systems 100 (2019): 569-578.

[5] Shynu, P. G., Varun G. Menon, R. Lakshmana Kumar, Seifedine Kadry, and Yunyoung Nam. "Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing." IEEE Access 9 (2021): 45706-45720.

[6] Al Omar, Abdullah, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. "Privacy-friendly platform for healthcare data in cloud based on blockchain environment." Future generation computer systems 95 (2019): 511-521.

[7] Ngabo, Desire, Dong Wang, Celestine Iwendi, Joseph Henry Anajemba, Lukman Adewale Ajao, and Cresantus Biamba. "Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things." Electronics 10, no. 17 (2021): 2110.

[8] ElRahman, Sahar A., and Ala Saleh Alluhaidan. "Blockchain technology and IoT-edge framework for sharing healthcare services." Soft Computing 25, no. 21 (2021): 13753-13777.

[9] Kumar, Randhir, and Rakesh Tripathi. "Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology." the Journal of Supercomputing (2021): 1-40.

[10] Ray, Partha Pratim, Biky Chowhan, Neeraj Kumar, and Ahmad Almogren. "BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem." IEEE Internet of Things Journal 8, no. 13 (2021): 10857-10872.

[11] Ahmad, Israr, Saima Abdullah, and Adeel Ahmed. "IoT-fog-based healthcare 4.0 system using blockchain technology." The Journal of Supercomputing 79, no. 4 (2023): 3999-4020.

[12] Fugkeaw, Somchart, Leon Wirz, and Lyhour Hak. "Secure and Lightweight Blockchain-enabled Access Control for Fog-Assisted IoT Cloud based Electronic Medical Records Sharing." IEEE Access (2023).

[13] Fernández-Caramés, Tiago M., Iván Froiz-Míguez, Oscar Blanco-Novoa, and Paula Fraga-Lamas. "Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care." Sensors 19, no. 15 (2019): 3319.

[14] Nasir, Muhammad Umar, Safiullah Khan, Shahid Mehmood, Muhammad Adnan Khan, Atta-Ur Rahman, and Seong Oun Hwang. "IoMT-based osteosarcoma cancer detection in histopathology images using transfer learning empowered with

 DOI : 10.35291/2454-9150.2024.0135

blockchain, fog computing, and edge computing." Sensors 22, no. 14 (2022): 5444.

[15] Mayer, André Henrique, Vinicius Facco Rodrigues, Cristiano André da Costa, Rodrigo da Rosa Righi, Alex Roehrs, and Rodolfo Stoffel Antunes. "Fogchain: a fog computing architecture integrating blockchain and internet of things for personal health records." IEEE Access 9 (2021): 122723-122737.

[16] Alam, Shadab, Mohammed Shuaib, Sadaf Ahmad, Dushantha Nalin K. Jayakody, Ammar Muthanna, Salil Bharany, and Ibrahim A. Elgendy. "Blockchain-based solutions supporting reliable healthcare for fog computing and internet of medical things (IoMT) integration." Sustainability 14, no. 22 (2022): 15312.

[17] Liu, Yanhui, Jianbiao Zhang, and Jing Zhan. "Privacy protection for fog computing and the internet of things data based on blockchain." Cluster Computing 24 (2021): 1331-1345.

[18] Baucas, Marc Jayson, Petros Spachos, and Konstantinos N. Plataniotis. "Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare." IEEE Transactions on Computational Social Systems (2023).

[19] Qu, Youyang, Longxiang Gao, Tom H. Luan, Yong Xiang, Shui Yu, Bai Li, and Gavin Zheng. "Decentralized privacy using blockchain-enabled federated learning in fog computing." IEEE Internet of Things Journal 7, no. 6 (2020): 5171-5183.

[20] Mohammed, Mazin Abed, Dheyaa Ahmed Ibrahim, and Karrar Hameed Abdulkareem. "Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment." Journal of King Saud University-Computer and Information Sciences 35, no. 1 (2023): 1-12.

[21] Costa, Humberto Jorge De Moura, Cristiano Andre Da Costa, Rodrigo Da Rosa Righi, Rodolfo Stoffel Antunes, Juan Francisco De Paz Santana, and Valderi Reis Quietinho Leithardt. "A fog and blockchain software architecture for a global scale vaccination strategy." IEEE Access 10 (2022): 44290-44304.

[22] Wazid, Mohammad, Ashok Kumar Das, Sachin Shetty, Joel JPC Rodrigues, and Mohsen Guizani. "AISCM-FH: AI-Enabled Secure Communication Mechanism in Fog Computing-Based Healthcare." IEEE Transactions on Information Forensics and Security 18 (2022): 319-334.

[23] Dammak, Bouthaina, Mariem Turki, Saoussen Cheikhrouhou, Mouna Baklouti, Rawya Mars, and Afef Dhahbi. "Lorachaincare: An iot architecture integrating blockchain and lora network for personal health care data monitoring." Sensors 22, no. 4 (2022): 1497.

[24] Al Omar, Abdullah, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. "Privacy-friendly platform for healthcare data in cloud based on blockchain environment." Future generation computer systems 95 (2019): 511-521.

[25] Egala, Bhaskara S., Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control." IEEE Internet of Things Journal 8, no. 14 (2021): 11717-11731.

[26] Donawa, Alyssa, Inema Orukari, and Corey E. Baker. "Scaling blockchains to support electronic health records for hospital systems." In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0550-0556. IEEE, 2019.

[27] Xu, Jie, Kaiping Xue, Shaohua Li, Hangyu Tian, Jianan Hong, Peilin Hong, and Nenghai Yu. "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data." IEEE Internet of Things Journal 6, no. 5 (2019): 8770-8781.

[28] Haux, Reinhold. "Medical informatics: past, present, future." International journal of medical informatics 79, no. 9 (2010): 599-610.

[29] Thakkar, Minal, and Diane C. Davis. "Risks, barriers, and benefits of EHR systems: a comparative study based on size of hospital." Perspectives in Health Information Management/AHIMA, American Health Information Management Association 3 (2006).

[30] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008).

[31] Digiteum, “Internet of medical things and medical software development,” 2020, [Online; accessed 5-June-2020]. https ://www.digit eum.com/inter net-medical-things- medical-software-development.

[32] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover and E. Hossain, "A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes," in IEEE Access, vol. 8, pp. 118433-118471, 2020, doi: 10.1109/ACCESS.2020.3004790.

[33] Shukla, Saurabh, Mohd Fadzil Hassan, Muhammad Khalid Khan, Low Tang Jung, and Azlan Awang. "An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment." PloS one 14, no. 11 (2019): e0224934.

 DOI : 10.35291/2454-9150.2024.0135

[34] Sen, Kabir C., and Kaushik Ghosh. "Designing Effective Crowdsourcing Systems for the Healthcare Industry." In Crowdsourcing: Concepts, Methodologies, Tools, and Applications, pp. 257-261. IGI Global, 2019.

[35] Waqar, Adeela, Asad Raza, Haider Abbas, and Muhammad Khurram Khan. "A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata." Journal of Network and Computer Applications 36, no. 1 (2013): 235-248.

[36] Bhuiyan, Mohammad Nuruzzaman, Md Mahbubur Rahman, Md Masum Billah, and Dipanita Saha. "Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities." IEEE Internet of Things Journal 8, no. 13 (2021): 10474-10498.

[37] Yadav, Umesh Chandra, and Syed Taqi Ali. "Ciphertext policy-hiding attribute-based encryption." In 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2067-2071. IEEE, 2015.

[38] Andriopoulou, Foteini, Tasos Dagiuklas, and Theofanis Orphanoudakis. "Integrating IoT and fog computing for healthcare service delivery." Components and services for IoT platforms: Paving the way for IoT standards (2017): 213-232.

[39] Mokhtari, Ghassem, Amjad Anvari-Moghaddam, and Qing Zhang. "A new layered architecture for future big data-driven smart homes." Ieee Access 7 (2019): 19002-19012.

[40] Harbi, Yasmine, Zibouda Aliouat, Allaoua Refoufi, and Saad Harous. "Recent security trends in internet of things: A comprehensive survey." IEEE Access 9 (2021): 113292-113314.

[41] Kharel, Jeevan, Haftu T. Reda, and Soo Y. Shin. "An architecture for smart health monitoring system based." Journal of Communications 12, no. 4 (2017): 228-233.

[42] Debe, Mazin, Khaled Salah, Muhammad Habib Ur Rehman, and Davor Svetinovic. "Blockchain-based decentralized reverse bidding in fog computing." IEEE Access 8 (2020): 81686-81697.

[43] Wazid, Mohammad, Ashok Kumar Das, Neeraj Kumar, Mauro Conti, and Athanasios V. Vasilakos. "A novel authentication and key agreement scheme for implantable medical devices deployment." IEEE journal of biomedical and health informatics 22, no. 4 (2017): 1299-1309.

[44] Wazid, Mohammad, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, and Willy Susilo. "Secure remote user authenticated key establishment protocol for smart home environment." IEEE Transactions on Dependable and Secure Computing 17, no. 2 (2017): 391-406.

[45] Wazid, Mohammad, Ashok Kumar Das, Neeraj Kumar, and Athanasios V. Vasilakos. "Design of secure key management and user authentication scheme for fog computing services." Future Generation Computer Systems 91 (2019): 475-492.

[46] Li, Daming, Zhiming Cai, Lianbing Deng, Xiang Yao, and Harry Haoxiang Wang. "Information security model of block chain based on intrusion sensing in the IoT environment." Cluster computing 22 (2019): 451-468.

[47] Tseng, Lewis, Xinyu Yao, Safa Otoum, Moayad Aloqaily, and Yaser Jararweh. "Blockchain-based database in an IoT environment: challenges, opportunities, and analysis." Cluster Computing 23 (2020): 2151-2165.

[48] Li, Hui, Lishuang Pei, Dan Liao, Xiong Wang, Du Xu, and Jian Sun. "BDDT: use blockchain to facilitate IoT data transactions." Cluster Computing 24 (2021): 459-473.

[49] Ma, Mingxin, Guozhen Shi, and Fenghua Li. "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario." IEEE access 7 (2019): 34045-34059.

[50] Alfandi, Omar, Safa Otoum, and Yaser Jararweh. "Blockchain solution for iot-based critical infrastructures: Byzantine fault tolerance." In NOMS 2020-2020 IEEE/IFIP network operations and management symposium, pp. 1-4. IEEE, 2020.

[51 Mohanta, Bhabendu Kumar, Debasish Jena, Somula Ramasubbareddy, Mahmoud Daneshmand, and Amir H. Gandomi. "Addressing security and privacy issues of IoT using blockchain technology." IEEE Internet of Things Journal 8, no. 2 (2020): 881-888.

[52] Zhaofeng, Ma, Wang Xiaochang, Deepak Kumar Jain, Haneef Khan, Gao Hongmin, and Wang Zhen. "A blockchain-based trusted data management scheme in edge computing." IEEE Transactions on Industrial Informatics 16, no. 3 (2019): 2013-2021.

 DOI : 10.35291/2454-9150.2024.0135