International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 10 | Oct - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Data Privacy and Security Enhancement in Internet of Things Network using Blockchain

Abhishek Gupta[1],Dr. Arun Sahayadhas[2], Aved Tiwari[3]
Ph.D. Student[1], Professor[2], Teacher[3]
Computer Science and Engineering[1,2]
Vels Institute of Science of Technology and Advanced Studies[1,2], Tribal Department[3]

Abstract

The entire Internet of Things (IoT) industry is anticipating advancements in network architecture and the creation of novel security methods that will make it possible to control and access Internet of Things (IoT) devices in a flexible, reliable and secure manner. Smart devices are susceptible to assaults due to low processing power and storage capacity because current security or cryptography techniques are ineffective. Blockchain technology is used in this project along with Internet of Things (IoT) for security authentication and verification purposes.
Blockchain's decentralization, anonymity, and proof-of-security features can stop centralized servers from colluding and collapsing in a single spot due to single point failure. In this project, a novel Multi-Input Data Concatenation (MIDC) technique is implemented to concatenate the multiple inputs for optimizing the blockchain storage. Here, the blockchain network checks for authenticity when a user requests access and then approves the request based on the data that has been stored. The integration of Blockchain into the Internet of Things (IoT) system can be able to remove the barriers preventing the advancement of Internet of Things (IoT) design and security. The proposed work outperforms existing cutting-edge methods by offering enhanced security performance, decreased Central Processing Unit (CPU) utilization time and power consumption, decreased cost, and decreased memory usage.

Keywords: Advanced Encryption System, Blockchain, Encrypted Data, Multi-Input Data Concatenation, Security authentication.

1. Introduction: -

The Internet of Things (IoT) is an emerging medium that joins intelligent, self-configuring "things" to provide a dynamic, effective network for collaboration and interaction. A cutting-edge technology called cloud computing enables networked nodes to share shared resources as needed under a subscription-based business model. Resources can be anything from a straightforward software program to a platform required for an initiative's progress to the network itself, which uses the Internet as its backbone. Cloud computing could manage concurrent inquiries from multiple tenants and is extremely scalable, changing, and flexible [1]. The adaptability of the cloud creates a number of network and data risk factors because, in a cloud-based setting, the majority of client data is transferred to data centers dispersed throughout the network's infrastructure where it is physically stored.

As a result, an enterprise's or client's information falls under the control of the service supplier, which creates the possibility of unforeseen security attacks and flaws when it is transmitted and used [2]. A distributed database known as blockchain is a recent invention in the world of information technology. The three basic standards for blockchain identification and availability are connection, private or approved, and public or less permitted. The most significant and distinctive aspect of the blockchain idea is that all of the stored data is completely secure inside each block of the blockchain's operations. Consistency, reliability, and acceptance of errors are its decentralized consensus algorithm's three key characteristics [4]. The Blockchain provides information origin, ensuring the accuracy of the data. Data blocks that have been encoded are used to store every exchange and data. The standards of the Blockchain technology comprise timestamps, cryptographic data, and client record information. The protocol circulates throughout the system; infrastructure; nevertheless, just the nodes for whom it was designed are able to use it, even if it may be visible among all related sites. The whole obligation of data transports, processing, and/or storing ought to come under the purview of the Blockchain-based cloud architecture. Anyone who addresses the Blockchain is going to able to understand what is unfamiliar with the data [6].

2. Methodology

The research focus on the providing the data privacy and security in IoT network using blockchain. The major goal is to guarantee the security and uphold the validity of substantial quantities of data related to the smart hospital. Researcher suggest building a solution based on blockchain technology to accomplish this, which includes the Solidity programming language and the Ganache blockchain network. The strategy calls for storing smart hospital data in the blockchain network or a de-centralised storage system, as well as modifying existing technology to match the needs. In this study, the Multi-Input Data Concatenation (MIDC) approach is used to integrate all the inputs before encryption. Instead of encoding each input separately, this approach concatenates the many inputs into one encrypted message. Data concatenation is used to create the distinct hash for each block on the blockchain. The contents from the current block and the block preceding it are combined to create the hash. Blockchain bridges facilitate communication between two blockchain networks by assisting with the mobility of data and digital assets.

This process optimizes the blockchain retention for storing information, which is its main advantage. As a result, research can keep a lot of data, and it also guards against corrupt or destruction of information. The Internet of Things (IoT) sensed data collected form the smart hospital is encrypted using the Advanced Encryption System (AES) encryption algorithm and then passed to the proof of work (PoW) process. The proof of work (PoW) verifies the request send by the user and this process take place at the blockchain network. When the user sends the request for access the proof of work verifies the access request. Either the request gets accepted or denied, if the request is accepted the decrypted data is send to the user on the other side if the request is denied the access get rejected. The above Fig.1 represent the overall work flow of proposed framework and the detail procedure is mentioned below.

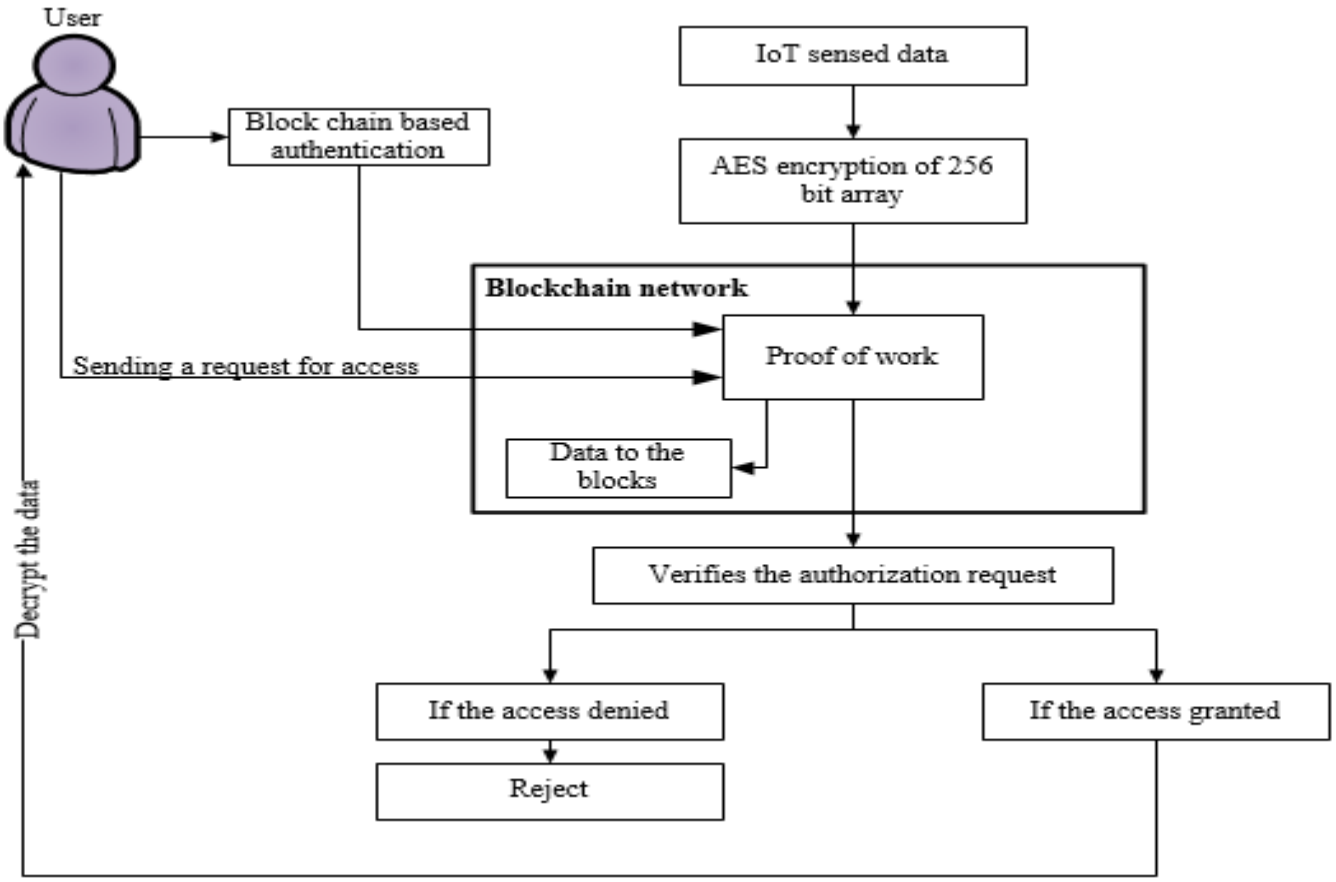

Figure 1: **Proposed Framework**

2.1 Proof of work

The most often used consensus technique in active blockchains is the proof of work (PoW) method. PoW was first used by the digital currency and operates under the premise that each peer casts a vote using his "computing power" by resolving proof-of-work cases and creating the necessary bits. Blockchain technology employs the consensus algorithm known as proof of work. Mining is the process of completing a difficult computing job in order to add additional blocks. based in Tel Aviv According to Proof Work, medical data will eventually be owned and managed by patients through a decentralised system with blockchain security. One of those most promising applications of the blockchain system is in the healthcare sector. Medical information may be found, located, and then directly exchanged between parties using blockchain technology [24].

- Energy Consumption: Simple Proof of Work systems consistently have the greatest rates of utilization of energy.
- Fairness: The highest levels of fairness are seen in absolute proof of work models, wherein input is dispersed equally and fairly among all nodes participating in data processing. With pure proof of work, the division of data generations is likewise fairly even.
- Reliability of the system: Absolute proof of work solutions have very high efficiency and dependability when it comes to processing data or resolving the equations that guarantee precise block production. Additionally, the reliability is consistent every time and doesn't change much.

Proof of work is extremely safe when contrasted with another implementation. Even a well-written proof of work blockchain, nevertheless, has numerous vulnerabilities. The present investigation and additional research in assessment of performance have

determined that Proof of Work Blockchain provides the highest level of equality and dependability. However, out of all the Blockchain technologies, Proof of Work uses the most energy. Finally, after the Proof of Work (PoW) process the authorization request send by the user is verified. If the requested is accepted the decrypted data is send to the user or else the access is rejected [25].

3. Result and discussion

The developer can create, launch, and test their DApp in a safe and predictable context using Ganache's. It has the ability to provide users with personal blockchains for DApp creation. MetaMask is an encrypted (digital) bank and entry point to blockchain apps that separates clients from their surroundings on the website while allowing them to access their accounts, keys, and currencies in a wide range of methods, including a hardware wallet. It is accessible as a browser extension and a mobile application. Microsoft created the free source-code editor Visual Studio Code for Windows, Linux, and macOS. A JavaScript package called React is used to create user interfaces. The declarative nature of this library makes the code more consistent and troubleshoot. Node.js is an event-driven, asynchronous JavaScript runtime created for building scalable online applications. In contrast to WEB 1.0 and WEB 2.0, WEB 3.0 emphasizes decentralization

and adds several new elements including verifiability, self-government, permission lessness, and distribution. An HTTP client for the browser and node.js is called Axios. It is very helpful to carry out CRUD processes and is employed to send asynchronous HTTP requests to APIs.

3.1 Encryption Comparison

Large datasets could be encrypted more rapidly and effectively thanks to the MIDC AES encryption technique. The data is encrypted and concatenated into separate blocks using this approach. This technique allows the data to be processed in parallel, considerably accelerating the encryption process. The fact that the MIDC-AES encryption process offers greater security than conventional AES encryption is having another benefit. The multi-input data concatenation AES encryption process is more adaptable than conventional AES encryption in addition to these benefits. The benefit of the MIDC AES mechanism over the AES technique is that while combined data encryption uses less memory, separately encrypted data uses more memory and the Table 1 presents the comparison of AES and MIDC-AES encryption mechanism.

Table 1: AES and MIDC-AES Encryption Comparison:-

	Text to be encrypted	**Secret key size (bits)**	**Encrypted data size (Bytes)**	**Total data size (Bytes)**
AES encryption mechanism	12	128	24	96 bytes
	8	128	24	
	4	128	24	
	2	128	24	
MIDC-AES encryption mechanism	12842	128	24	24 bytes

Four text values (12, 8, 4, and 2) that have been encrypted using AES and MIDC-AES are displayed in the table. The data is 96 bytes in size when using AES encryption (24 bytes for each text byte), and 24 bytes in size when using MIDC-AES encryption. It is evident from the above table that when each data is encrypted separately, the size of the data increases, however the size of the data decreases when the many data are concatenated before encryption. As a result, the MIDC-AES encryption process uses a small amount of storage to store the data.

Table 2: Average Encryption time Comparison

Method	Average Encryption time (ms)	Reference
AES-CBC	1.56	[26]
AES-SHA	32.95	[27]
AES-256	11.75	[28]
Proposed (MIDC-AES)	*1.14*	-

3.2 Comparison of end-to-end delay

The time required for a packet to move from origin to target over a network is known as a one-way delay (OWD), also referred to as an end-to-end delay. This expression, which is frequently employed in IP network surveillance, differs from round-trip time (RTT) in that it only accounts for the distance travelled in one direction from origin to target. The following Table 3 shows the end-to-end delay comparison between the Ethereum blockchain and the proposed MIDC-AES approach.

Table 3: End-to-end delay Comparison

Method	End-to-end delay
Ethereum blockchain	0.11
Proposed (MIDC-AES)	0.08

3.3 Comparison of average power consumption: - Internet of Things (IoT) devices primarily take into account energy usage when creating records or updating health information in the blockchain. The following Table 4 shows the average power comparison of AES-CBC, AES-256 and Proposed (MIDC-AES).

Table 4: Average Power Consumption Comparison

Method	Average power consumption (mW)		Reference
	Encryption	Decryption	
AES-CBC	0.193	0.247	[26]
AES-256	0.235	0.346	[28]
Proposed (MIDC-AES)	0.172	0.194	-

4. Conclusion

Due to its eternity, independence, and complete transparency, the blockchain presents itself as an intriguing option for health data safety. People's identities and medical records will continue to be retained in confidence utilizing Blockchain as long as the system is secure. By eliminating inefficient and unwanted instrumentation, this groundbreaking solution will simplify the challenging billing procedure. It can also assist patients with uploading and permit authorized parties to examine medical documents. Block chain technology may offer a fresh approach for sharing healthcare data by improving the efficiency, dependability, and security of digital medical records. Researcher proposed to use Internet of Things (IoT) based blockchain technology regarding the transfer data transactions in an Internet of Things (IoT) medical system. For sensor networks that are wireless, several researchers offer various security protocols. On Wireless Sensor security systems, there nevertheless exist surprisingly few research publications. As a result, designing security protocols for wireless sensor should be driven primarily by the desire to make them as energy-efficient as possible. The approach would use a permissioned, consortium-managed blockchain to

carry out smart contracts that would assess data gathered by a patient's Internet of Things (IoT) healthcare equipment according to threshold values. It is clear that authentication is crucial for achieving safe communication in hospital (or other) networks. Because blockchain technology may be used to offer a straightforward and efficient communication platform, blockchain-based authentication methods are one current a pattern. The blockchain-based method aims to make it possible to securely capture data in a network of healthcare facilities with a wide range of geographic locations. In addition to recording information about the interaction on the blockchain for request verification, the smart contracts would send alerts to the patient and healthcare practitioners as necessary. To show the system's data flow, research programmed smart contracts in Solidity as a proof-of-work.

5. Future Works

We have worked on the data privacy and security enhancement in Internet of things network using blockchain, but it's speed can be further enhanced by modifying the internal processing unit on which Central Processing Unit (CPU) it is being deployed, the sample example-set is given in [30], So the further enhancement can be done at the hardware level on which it is being deployed. Apart from the same Built-In-Self-Test at the software level can be applied on the same, so that if any errors come on the same then it can be debugged by itself, the example-set for the same is given in [31]. Furthermore, the data-sets received by the proposed model can be stored in the Speed efficient Data ware house architecture so based on the same, knowledge discovery process can be faster, the example set is given in the [32],[33],[34].

Reference

[1] G. Zhang, X. Zhang, M. Bilal, W. Dou, X. Xu, and J. J. Rodrigues, "Identifying fraud in medical insurance based on blockchain and deep learning," Future Gener. Comput. Syst., vol. 130, pp. 140–154, 2022.

[2] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, and A. Refaey, "ssHealth: toward secure, blockchain-enabled healthcare systems," IEEE Netw., vol. 34, no. 4, pp. 312–319, 2020.

[3] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. Abd El-Latif, "DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems," IEEE Access, vol. 8, pp. 111223–111238, 2020.

[4] M. Du, Q. Chen, J. Chen, and X. Ma, "An optimized consortium blockchain for medical information sharing," IEEE Trans. Eng. Manag., vol. 68, no. 6, pp. 1677–1689, 2020.

[5] S. Chakraborty, S. Aich, and H.-C. Kim, "A Secure Healthcare System Design Framework using Blockchain Technology," in 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea (South): IEEE, Feb. 2019, pp. 260–264. doi: 10.23919/ICACT.2019.8701983.

[6] P. Hemalatha and others, "Monitoring and securing the healthcare data harnessing IOT and blockchain technology," Turk. J. Comput. Math. Educ. TURCOMAT, vol. 12, no. 2, pp. 2554–2561, 2021.

[7] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," Health Informatics J., vol. 25, no. 4, pp. 1398–1411, Dec. 2019, doi: 10.1177/1460458218769699.

[8] B. Sharma, R. Halder, and J. Singh, "Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption," in 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), IEEE, 2020, pp. 1–6.

[9] A. Rahman, Md. J. Islam, Md. Saikat Islam Khan, S. Kabir, A. I. Pritom, and Md. Razaul Karim, "Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network," in 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh: IEEE, Dec. 2020, pp. 1–6. doi: 10.1109/STI50764.2020.9350419.

[10] R. Arul, Y. D. Al-Otaibi, W. S. Alnumay, U. Tariq, U. Shoaib, and M. D. J. Piran, "Multi-modal secure healthcare data dissemination framework using blockchain in IoMT," Pers. Ubiquitous Comput., Feb. 2021, doi: 10.1007/s00779-021-01527-2.

[11] C. P. Jayabal and P. R. K. Sathia Bhama, "Performance analysis on Diversity Mining-based Proof of Work in bifolded consortium blockchain for Internet of Things consensus," Concurr. Comput. Pract. Exp., vol. 33, no. 16, Aug. 2021, doi: 10.1002/cpe.6285.

[12] H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An IoT blockchain architecture using oracles and smart contracts: the use-case of a food supply chain," in 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2019, pp. 1–6.

[13] F. Zhao, C. Li, and C. F. Liu, "A cloud computing security solution based on fully homomorphic encryption," in 16th International Conference on Advanced Communication Technology, Pyeongchang, Korea (South): Global IT Research Institute (GIRI), Feb. 2014, pp. 485–488. doi: 10.1109/ICACT.2014.6779008.

[14] F. Jamil, L. Hang, K. Kim, and D. Kim, "A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital," Electronics, vol. 8, no. 5, p. 505, May 2019, doi: 10.3390/electronics8050505.

[15] A. Jyoti and R. K. Chauhan, "A blockchain and smart contract-based data provenance collection and storing in cloud environment," Wirel. Netw., vol. 28, no. 4, pp. 1541–1562, May 2022, doi: 10.1007/s11276-022-02924-y.

[16] D. Li, W. Peng, W. Deng, and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT," in 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou: IEEE, Jul. 2018, pp. 1–6. doi: 10.1109/ICCCN.2018.8487449.

[17] S. Hong, "P2P networking based internet of things (IoT) sensor node authentication by Blockchain," Peer--Peer Netw. Appl., vol. 13, no. 2, pp. 579–589, Mar. 2020, doi: 10.1007/s12083-019-00739-x.

[18] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," IEEE Sens. J., vol. 16, no. 5, pp. 1368–1376, 2015.

[19] Y. Qian et al., "Towards decentralized IoT security enhancement: A blockchain approach," Comput. Electr. Eng., vol. 72, pp. 266–273, Nov. 2018, doi: 10.1016/j.compeleceng.2018.08.021.

[20] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," Clust. Comput., vol. 23, no. 3, pp. 2067–2087, Sep. 2020, doi: 10.1007/s10586-020-03058-6.

[21] M. Tahir, M. Sardaraz, S. Muhammad, and M. Saud Khan, "A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics," Sustainability, vol. 12, no. 17, p. 6960, Aug. 2020, doi: 10.3390/su12176960.

[22] F. Jamil, L. Hang, K. Kim, and D. Kim, "A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital," Electronics, vol. 8, no. 5, p. 505, May 2019, doi: 10.3390/electronics8050505.

[23] M. Naz et al., "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System," Sustainability, vol. 11, no. 24, p. 7054, Dec. 2019, doi: 10.3390/su11247054.

[24] C. P. Jayabal and P. R. K. Sathia Bhama, "Performance analysis on Diversity Mining-based Proof of Work in bifolded consortium blockchain for Internet of Things consensus," Concurr. Comput. Pract. Exp., vol. 33, no. 16, Aug. 2021, doi: 10.1002/cpe.6285.

[25] M. Roy and M. Singh, "Analytical Study of Blockchain Enabled Security Enhancement Methods for Healthcare Data," IOP Conf. Ser. Mater. Sci. Eng., vol. 1131, no. 1, p. 012002, Apr. 2021, doi: 10.1088/1757-899X/1131/1/012002.

[26] S.-W. Lee and K.-B. Sim, "Design and hardware implementation of a simplified DAG-based blockchain and new AES-CBC algorithm for IoT security," Electronics, vol. 10, no. 9, p. 1127, 2021.

[27] V. Goyal and C. Kant, "An effective hybrid encryption algorithm for ensuring cloud data security," in Big Data Analytics: Proceedings of CSI 2015, Springer, 2018, pp. 195–210.

[28] E. P. Nugroho, Rizky Rachman Judhie Putra, and Iman Muhamad Ramadhan, "SMS authentication code generated by Advance Encryption Standard (AES) 256 bits modification algorithm and One time Password (OTP) to activate new applicant account," in 2016 2nd International Conference on Science in Information Technology (ICSITech), Balikpapan, Indonesia: IEEE, Oct. 2016, pp. 175–180. doi: 10.1109/ICSITech.2016.7852629.