Journal of Autonomous Intelligence (2024) Volume 7 Issue 2
doi: 10.32629/jai.v7i2.1073

ORIGINAL RESEARCH ARTICLE

An efficient framework for secure data transmission using blockchain in IoT environment

Shyama Barna Bhattacharjee[1,*], Shivam Gangwar[2], Manish Kumar[3], Kirti Saini[4], Rashmi Saini[5], Shivani Chauhan[4], Krishna Pandey[4], Richard Essah[6], Nitin Goyal[7]

[1] *Computer Science and Engineering Department, University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra 136119, India*

[2] *University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra 136119, India*

[3] *Zakir Husain Delhi College, Delhi University, Delhi 110002, India*

[4] *Electronics and Communication Engineering Department, University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra 136119, India*

[5] *Institute of Instrumentation Engineering, Kurukshetra University, Kurukshetra 136119, India*

[6] *Department of Computer Science and Engineering, Chandigarh University, Punjab 140413, India*

[7] *Department of Computer Science and Engineering, School of Engineering and Technology, Central University of Haryana, Mahendragarh 123031, India*

*** Corresponding author:** Shyama Barna Bhattacharjee, shyamabarna891@gmail.com

ABSTRACT

The secure and efficient sharing of data has been recognised as a significant concern in Internet of Things (IoT)-enabled smart systems, including smart cities, smart agriculture, and smart health applications. Smart systems utilise a substantial quantity of IoT devices, which in turn generate a significant volume of data. Internet of Things (IoT) devices typically possess constrained storage and processing capacities, making the implementation of security measures on such devices a difficult task. This paper presents a framework for secure data transmission using blockchain (SDTUB) for blockchain-based IoT systems, with a focus on enhancing data security. The use of clustered authorization aims to enhance the interoperability of IoT authorization. The central blockchain is employed for permission purposes concerning cluster management nodes, whereas the regional blockchain suffices for authorization of regular nodes. The proposed mechanism is implemented using MATLAB, and the performance is analysed using performance metrics such as energy consumption and objective value. In the proposed mechanism, the energy consumption is low compared to the AuBWSN technique.

Keywords: IoT; blockchain; security; attacks; authentication

ARTICLE INFO

Received: 28 July 2023
Accepted: 11 October 2023
Available online: 21 December 2023

1. Introduction

IoT refers to the integration of internet connectivity with various embedded devices within the realm of information technology. The establishment of wireless connectivity between devices has the potential to revolutionize interactions between systems, offering novel opportunities for control, tracking, and the integration of advanced service functionalities[1]. IoT devices are inherently designed with specific limitations, which impose restrictions on the available resources and performance capabilities in comparison to network devices found in enterprise environments. When developing a management and monitoring system for IoT

devices, it is essential to consider this aspect. The heterogeneity of IoT devices, employed for diverse purposes, necessitates distinct configurations and offers varying degrees of monitoring capabilities. The presence of diverse devices within enterprise network environments allows for the modification of current network monitoring and management systems to accommodate the implementation of the IoT[2].

Enterprise networks and public access networks serve as integral communication infrastructures within organizations and communities, facilitating widespread connectivity on a global scale. The enterprise networks sector is undergoing continuous development and is receptive to innovations in order to enhance connectivity among nodes and ensure greater security. The primary area of emphasis for the key innovation should revolve around three critical aspects: enhancing network performance, reinforcing security measures, and minimizing maintenance expenses through the implementation of blockchain technology[3].

Simultaneously, the investigation of network access security requirements through the utilization of blockchain technology constitutes a distinct area of study. The specifications are contingent upon numerous factors, primarily influenced by the attributes of the network, such as its topology[4]. However, network monitoring plays a crucial role as a database utilized for security control.

A blockchain, alternatively referred to as a distributed shared record, is a database consisting of records that cannot be altered, and is protected through the use of cryptographic techniques. This technology facilitates the transfer and retention of digital assets without requiring the involvement of intermediaries[5]. Devices that retrieve a configuration file from a centralized server must place trust in the authority of the server. In the event that this authority is compromised, the device becomes susceptible to vulnerabilities. The presence of a blockchain eliminates the necessity for a central authority. Devices engage in direct asset exchange with one another, operating in a peer-to-peer manner.

The blockchain possesses certain fundamental characteristics that differentiate it from a conventional database. Firstly, it is inherently distributed. Furthermore, it is important to note that the records stored in the blockchain possess the characteristic of immutability, rendering them impervious to deletion or modification. By doing so, it would compromise the validity. The process of updating records necessitates the creation of a new record rather than modifying an existing one.

In this manner, a comprehensive record of all modifications is securely maintained. The blockchain employs smart contracts, also known as chaincode, to guarantee the accurate implementation of predetermined business regulations. A smart contract refers to a computer program, functioning as an agreement, which is executed by nodes within the blockchain network to enable automation. Smart contracts are also employed for the purpose of managing configuration files within an IoT setting[6]. The utilization of blockchain technology is employed for the purpose of device identification.

Device identification is a crucial procedure aimed at confirming the authenticity of a specific device transmitting data, thereby enabling the recipient to ascertain the data's origin from the intended source. The process of identification plays a crucial role in guaranteeing the authenticity of data and mitigating potential risks arising from unauthorized devices that falsely claim their identity[7].

In this study, we present a novel protocol for identifying IoT devices by leveraging fuzzy extractors and incorporating timing information[8]. The protocol exhibits a high degree of accuracy in identifying an IoT device, and it offers compelling evidence of message authentication. In contrast to the current methodologies, the protocol being proposed exhibits minimal additional computational burden while producing a message authentication code. **Figure 1** depicts the fundamental design architecture for secure data transmission and data monitoring in IoT using blockchain. Here figure shows that devices

are authenticated with some access control techniques and data is transmitted using blockchain techniques in IoT. After authenticating with digital certificates, authorized network administrators can make changes to the device configurations stored in the blockchain[9].

As an alternative to traditional Public Key Infrastructure (PKI), a blockchain-based architecture may be used to maintain authentication certificates[10]. To reduce the possibility of human mistake being introduced into configuration stored in the blockchain, it is recommended that a syntax verification be used to confirm the validity of the new configuration. Each device may then use its unique identifier to determine whether or not the addition impacts its settings. The device then retrieves its encrypted configuration from the blockchain, decrypts it with its private key, and puts the changes into effect. Security and auditing teams may look up the history of all the modifications in the blockchain.

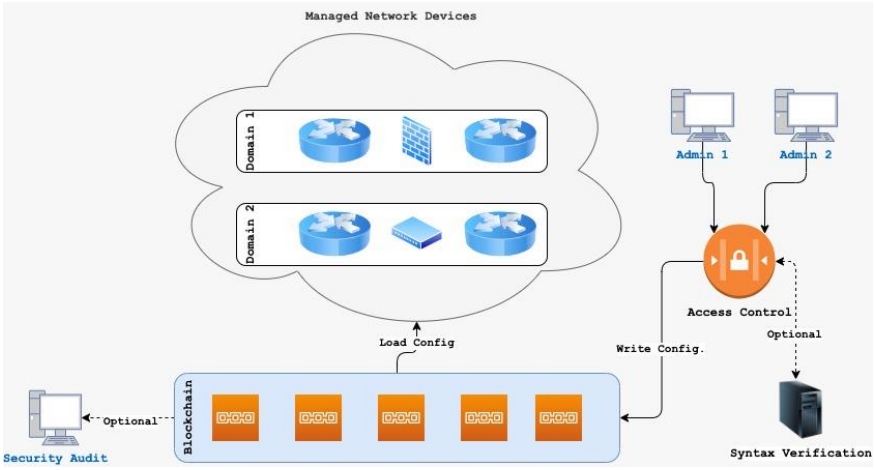

Figure 1. Architecture for secure data transmission using Blockchain.

The primary contributions of this paper are:

1) To provide role of block chain in secure data transmission in IoT based system.
2) To propose secure data transmission framework using blockchain for IoT.
3) To analyse performance of proposed framework with performance metrices such as energy consumption and objective value.

The manuscript provides a secure data transmission framework for IoT using blockchain technology. Initially, the introduction of block chain and its role for device management and secure data transmission were discussed; after that, a literature review of various existing papers related to block chain-based secure data management in the IoT was presented. Furthermore, it provides a system architecture, and a proposed framework has been presented. Thereafter, the results and discussion are presented, and at last, the conclusion of the paper is discussed.

2. Related work

In this section review of literature on secure data transmission in IoT using blockchain has been presented. The assessment of IoT privacy in conventional ways frequently adheres to standardized authentication protocols. Signature systems of this sort necessitate dependence on a reliable third-party entity, such as an identity authorization facility or a digital certificate, in order to mitigate the risk of a single-point failure. The security concerns associated with the IoT. However, it should be noted that the utilization of blockchain technology to address security difficulties is now in the experimental stage, and as a result, the most recent solutions based on blockchain still encounter a number of challenges. In contemporary investigation of IoT security, a significant portion of research focuses on blockchain

technology, primarily examining two key areas: the framework for securing IoT devices and the strategies employed to mitigate security risks. **Table 1** provides a comparison of the presented papers selected for literature with pros and cons.

Table 1. Comparison Table with pros and cons.

Author	Highlights	Pros	Cons
Zhang et al.[11]	Provides application-oriented block generation (AOBG) for IoT and blockchain integration.	Addresses specific needs of IoT applications.	Scalability Issues and poor resource utilization.
Gong et al.[12]	Introduced a framework for device administration using blockchain.	Enhances device management efficiency. Enables scalable firmware updates. Improves network security.	Cost affective and Privacy issues.
He et al.[13]	Proposed a privacy-preserving IoT device management scheme based on blockchain.	Effective access control based on time constraints and attributes. Capability for key revocation.	Complexity and energy consumption.
Wickström et al.[14]	Utilized smart contracts on Ethereum blockchain for IoT security.	Ensures sustained health of IoT networks.	Resource utilization is poor.
Loukil et al.[15]	Introduced a framework for managing IoT devices while ensuring anonymity using blockchain.	Provides device anonymity. Utilizes smart contracts for governance.	Poor scalability.
Novo[16]	Conducted a comparative analysis of IoT access control systems.	Examined latency and throughput of systems.	Only highlights access control techniques
Moon et al.[17]	Proposed a methodology for enhancing security and data integrity in home IoT systems using blockchain.	Offers protection against 51% assaults. Allows individual consensus rate establishment.	High latency and energy consumption.
Qureshi et al.[18]	Conducted a comprehensive analysis of blockchain technology in IoT.	Provides insights into blockchain's use in various IoT fields.	Interoperability issues.
Zhang et al.[19]	Proposed a blockchain-based fast and dynamic access control (FDAC) system for fog-assisted microgrid.	Recommends attribute-based access control for versatility and efficiency.	Poor scalability.
Rana et al.[20]	Conducted a comprehensive analysis of architectures in the BIoT field.	Highlights existing technologies, applications, problems, and prospects.	Energy consumption is high.
Herdem et al.[21]	Analyzed literature and patents in interconnected smart energy management sectors.	Utilized AI models for energy consumption prediction and resource optimization.	Poor scalability.
Rana et al.[22]	Explored the use of blockchain technology in the healthcare sector.	Addresses healthcare data security challenges.	Poor resource utilization/
Deebak et al.[23]	Proposed a trust-aware blockchain-based authentication system with privacy preservation.	Demonstrates improved user connectivity and communication metrics.	Energy consumption.
Kairaldeen et al.[24]	Conducted experiments to assess the scalability of a secure blockchain communication system.	Provides notable improvement in execution time.	Scalability and energy consumption.
Mubarakali[25]	Presented an approach to identification in WSNs using distributed blockchain technology.	Incorporates secure connections in communication scenarios.	Complexity.

Zhang et al.[11] introduced a method called application-oriented block generation (AOBG) that is designed for the integration of blockchain technology with the IoT. This scheme incorporates dynamic device management and conditional traceability to cater to the specific needs of IoT applications.

Furthermore, Gong et al.[12] introduced a framework for device administration that utilizes blockchain technology. This framework aims to enhance the efficiency of device management, enable scalable firmware updates, and improve resistance against assaults on smart city networks. This framework provides four mechanisms for managing devices and updating firmware, which are selected depending on the performance and needs of each device. These mechanisms include a bidirectional mechanism for conventional end nodes and a unidirectional technique for lightweight end nodes. This disparity enhances the efficiency of managing and securing network resources and devices. The blockchain technology is utilized to preserve the whole management history of each device, ensuring the security and resilience against any attacks. The transmission of firmware between the vendor and management node is facilitated using a smart contract implemented on the blockchain. Similarly, He et al.[13] introduced a scheme for managing IoT devices that prioritizes privacy preservation. This scheme is built upon blockchain technology and offers effective access control based on time constraints and attributes. Additionally, it has the capability for automated revocation of keys.

Furthermore, the approach proposed by Wickström et al.[14] involves the utilization of smart contracts on the Ethereum blockchain as a protocol to impose a security model. This model aims to ensure the sustained health of dispersed IoT networks throughout their existence. Moreover, Loukil et al.[15] introduced a framework for managing IoT devices while ensuring anonymity, utilizing blockchain technology. The proposed system involves the utilization of smart contracts to govern the operation of IoT devices. In the similar manner, Novo[16] conducted a comparative analysis of the suggested solution and existing access control systems in the context of the IoT. The latency and throughput rate of the systems were examined. also conducted an analysis of various configurations of our solution in order to optimize its scalability. However, Moon et al.[17] proposed a methodology for enhancing security and preserving data integrity in Home IoT systems by leveraging smart contracts inside a blockchain-based framework. Additionally, it proposes a method for individuals to safeguard themselves against 51% assaults by the establishment of their own consensus rate. Similarly, Qureshi and colleagues[18] conducted a comprehensive analysis of the existing blockchain technology and its present use in many fields of the IoT. Furthermore, Zhang et al.[19] proposed a blockchain-based fast and dynamic access control (FDAC) system for managing devices in a fog-assisted microgrid. To effectively represent a versatile, adaptable, and efficient fine-grained access control system, it is recommended to employ an attribute-based access control framework. However, Rana et al.[20] conducted a comprehensive analysis of several architectures in the field of BIoT, highlighting the existing technologies, applications, problems, and potential prospects. Similarly, Herdem et al.[21] conducted a comprehensive analysis of the literature and patents in four interconnected sectors, with the objective of offering a comprehensive understanding of their interrelationships and their potential integration within the context of smart energy management techniques. Artificial intelligence models are utilized to predict energy consumption and load patterns, while also optimizing resource allocation to ensure dependable performance and efficient utilization of energy resources. Thereafter, Rana et al.[22] examined the utilization of a nascent technology within the healthcare sector. Blockchain technology has the potential to address several challenges in the healthcare sector, such as drug traceability and medical record administration. The healthcare industry is currently seeing several challenges as a result of the susceptibility of healthcare data to security risks, including attacks on integrity, confidentiality, and availability. Furthermore, Deebak et al.[23] proposed a trust-aware blockchain-based seamless authentication with privacy-preserving (TAB-SAPP) system to address important concerns like privacy and security. The suggested TAB-SAPP introduces a unique approach to data traffic patterns by leveraging identity management. This approach aims to demonstrate the enhanced functionality of the

proposed mechanism in increasing users' connectivity and improving communication metrics, including packet delivery ratio and mobility speed. Furthermore, Kairaldeen et al.[24] conducted experiments to assess the scalability of their suggested system for secure blockchain communication. The researchers examined the execution of different dataset sizes, which were generated by transactions between nodes. The findings indicate that the utilization of the proposed data structure method, in conjunction with the SHA3 and AES-128 encryption algorithms, yields the most favorable execution time. This approach demonstrates a notable improvement in time optimization, with a minimum gain of 36% when compared to other techniques. Similarly, Mubarakali[25] presented a reliable approach to identification in WSNs by leveraging the distributed blockchain technology. In many communication scenarios, the hybrid model incorporates nodes that enable the establishment of secure connections. Within the blockchain network, user authentication is achieved by the identification of normal nodes. This process involves the utilization of local blockchain technology and the verification of chosen cluster nodes.

3. System architecture of proposed mechanism

Through the use of blockchain technology, the Internet of Things (IoT) enables the secure transfer of data between a distributed network of devices. In this study, we present a framework that uses blockchain technology to facilitate secure data transmission in IoT using blockchain. Through the use of blockchains, which record configuration changes made by network administrators and which devices then check for updates, administrators can exert indirect control on network devices.

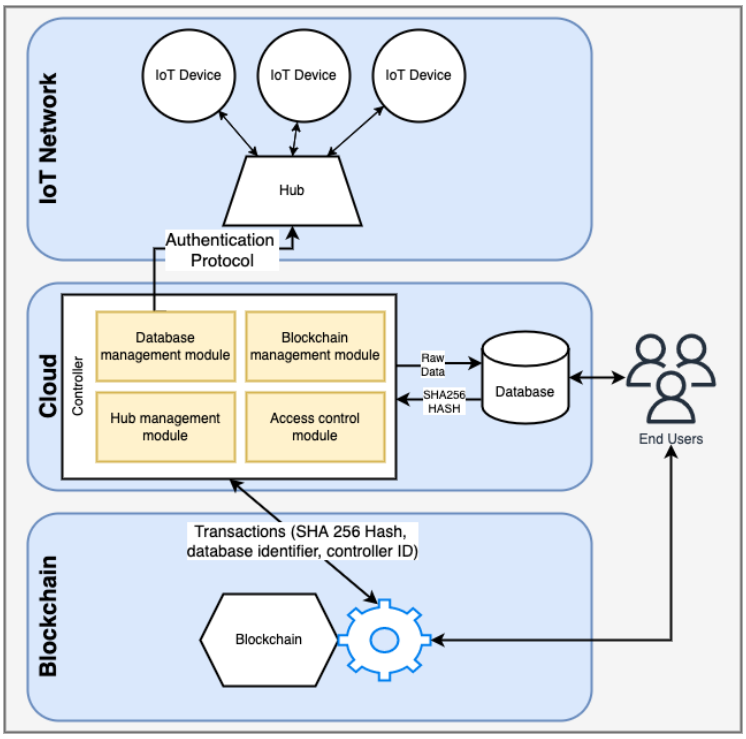

Figure 2. System framework of SDTUB framework.

The system under consideration depicted in **Figure 2** that comprises seven distinct entities, namely sensors, hubs, controller, cloud, database, blockchain, and users. The sensors in proposed system are lightweight devices that lack the necessary computational capacity for cryptographic computations. Hubs possess constrained processing and storage capacities, yet exhibit comparatively greater strength when compared to IoT devices. Solutions that combine IoT (Internet of Things), Blockchain, and cloud

computing have the potential to significantly improve application-level security, scalability, and trust. Keeping IoT data secure and unchangeable is a top use case for blockchain integration. IoT data and devices are more secure when protected by blockchain technology. Dashboards and other management tools hosted in the cloud make it possible for customers to keep tabs on their IoT gadgets and blockchain transactions in real time. IoT data may be put to good use with the help of cloud-based analytics, and its validity and dependability can be guaranteed with the help of blockchain technology.

The controller serves as the primary component of the system, fulfilling various functions and engaging in interactions with the hubs, database, and blockchain.

4. Proposed approach in IoT

The proposed SDTUB mechanism presents an authentication solution for the IoT that aims to defines the entire system against a range of network attacks. **Figure 3** illustrates the working of suggested approach that comprise the authentication process within the established framework. A powerful solution to the problems associated with the authentication of Internet of Things (IoT) devices can be found in the combination of local and global blockchains. For the purposes of this article, "local blockchain" will refer to a blockchain network that is internal to a single company or geographical region. It gives people a sense of agency, scalability, and privacy in that ecosystem. Blockchains that are public or run by a consortium may not be applicable on a global scale, but there is another type of blockchain that is: the global blockchain. It's open to a wide variety of users and can facilitate distributed, trustworthy information sharing. The integration of regional and international blockchains, however, creates new problems. overcome obstacles Interoperability between regional and international blockchains can be achieved through the adoption of standardised blockchain protocols and communication standards. This ensures that various blockchain networks can successfully interact with one another. Furthermore, the use of a global blockchain to record periodic hashes or summaries of data that is stored and confirmed on local blockchains can be implemented. This preserves openness without increasing the strain on the worldwide blockchain.

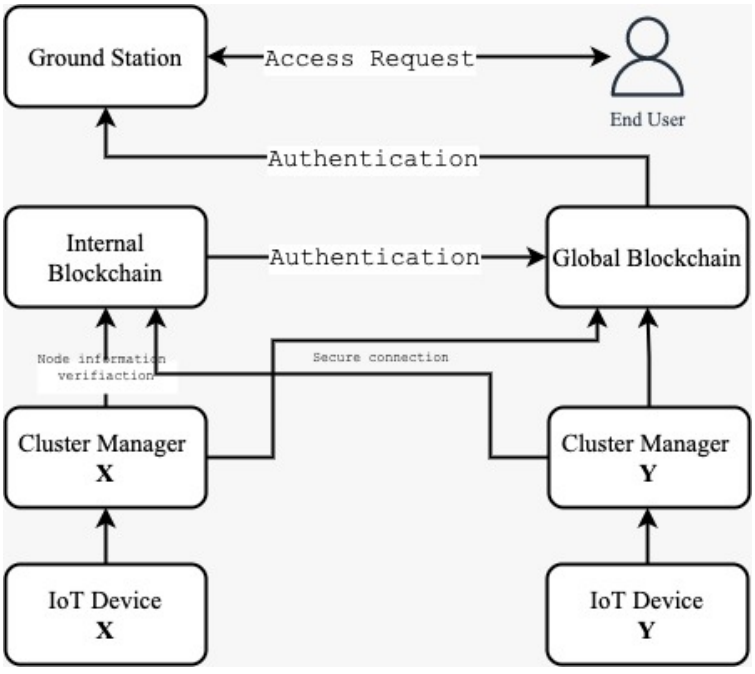

Figure 3. Working framework of proposed mechanism.

The diverse metadata associated with the nodes has been kept within the blockchain, hence facilitating automated management by the blockchain controller. The metadata encompasses several elements, including as the Gs_ID (Ground Station ID), C_ID (Cluster ID), S_Key (Key Pair), and tags. These components play a crucial role in facilitating the maintenance of data connections. The management of metadata will be overseen by the primary blockchain, which is responsible for ensuring safe communication and authentication.

In this section, we will provide a more comprehensive explanation of the processes involved in the proposed authentication approach based on blockchain technology. Each sensor node is issued a unique S_ID (sensor ID) upon its connection to the network cluster. The primary task of the ground station manager is to ascertain the membership of all sensor nodes within a given cluster. Each node, denoted as n_j, has been associated with its respective network identifier, referred to as A_j. The ground station has utilized a hash function to produce an identification (ID) for the node. This ID, denoted as NID_j, is obtained by applying the hash function over the physical address, represented as Aj. In this context, the digital IDs assigned to several categories of nodes, namely sensor nodes, cluster management nodes, and ground stations, are denoted as $SNID$, $CMID$, and GID, respectively. The ground station has created a set of keys, consisting of a public key (k_{pub}) and a private key (k_{pri}).

A user (acting on behalf of the device) communicates with the cloud in order to complete the registration process. The user first produces an identifier (ID), a timetable (T_s), auxiliary information (X), and a secret key (s_k). To register a device with the cloud, the user transmits (ID,s_k,X). After a device is registered, its (ID,s_k,X) is saved in the cloud and made available to a controller. This protocol is depicted below.

User's end:

$$(X, Y) \leftarrow Gen(T_s), \qquad Where\ X = (s, r)$$
$$s_k \leftarrow KeyGen(R)$$

Cloud end:

$$Store(ID, s_k, X)$$

Finally, the ground station is responsible for allocating an identification label to the sensor nodes, including all previously specified identifiers. The identification of the sensor node is accomplished by the utilization of the ground station produced identity, which is required to be in the format of SNID/CMID.

The distribution of cluster heads aims to effectively allocate clusters throughout the network in order to provide a comprehensive network design. The approach involves establishing a connection between the identifying information of the valid node and its corresponding ground station and cluster management nodes, and subsequently storing this information in the global blockchain. The default node contains the fundamental framework. The allocation of value to sensor nodes is not a necessary need. The variable SS denotes the remaining condition of the node in situations such as destruction, invasion, depletion, and other issues that may arise, which should be disregarded.

The process of evaluating the functionality and performance of sensor nodes is carried out using a decentralized record technology known as a local blockchain. In the context of a cluster management system, it is observed that each sensor node has the capability to join just a single cluster system, even while there are several cluster manager nodes present. After carefully considering the rules, the chosen cluster system necessitates the popular node to publish the configuration connection request via the Configuration Application. The initial step in the validation process of the management node involves

verifying the accuracy and dependability of the clock. Once a certain level of trustworthiness is achieved, the authentication transfer is established within the internal blockchain network.

If all of the aforementioned methods prove unsuccessful in verification, the response will be returned. Once all procedures affecting to organizational improvement are enhanced, the fundamental network node has the capability to transmit the identity information of the ordinary node to the public database for the purpose of preservation, utilizing the aforementioned format. Additionally, it may distribute a notification confirming the successful completion of the verification process. The local network determines that the ordinary node will establish a connection with the cluster system.

The flowchart of the proposed framework is depicted in **Figure 4**. In the proposed system, nodes are initially deployed in a simulated scenario. Subsequently, security parameters are allocated. The process of establishing a fixed security parameter. The initialization of security parameters for the ground station is mostly the responsibility of the station management module. The initialization of these settings is performed consistently over the duration of the session for all IoT devices. In addition, the concept of blockchain integration. In the subsequent phase, it is vital to integrate all sensor nodes within the IoT through the utilization of a worldwide blockchain.

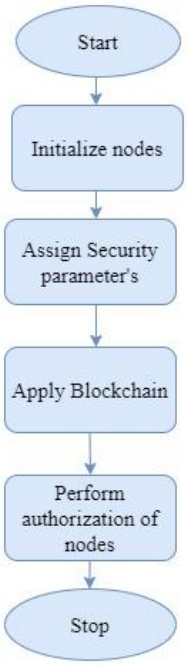

Figure 4. Flow chart of proposed framework.

In the subsequent phase, the process of authorisation is conducted, wherein authenticated nodes engage in ongoing communication of their identification information. This enables them to get authorization to participate in the IoT through the global blockchain mechanism.

5. Result and discussion

This section provides simulation results and discussion. To simulate proposed mechanism MATLAB has been used. The simulation has been performed five times in order to achieve optimal results. The parameters used for simulation has been depicted in **Table 2**. Here **Table 2** provides the parameters such as initial energy of nodes, size of messages and simulation area. This section discusses the efficient implementation of an authentication system that successfully verifies the authenticity of valid nodes attempting to access the network and then grants them access while denying unauthorized

entities. The nodes that do not meet the criterion for scalability are incorrect. Semi-repudiation non-repudiation pertains to the assurance that the actions and communications undertaken by individuals or entities will not be subject to dispute from consumers and computer systems.

The methodology is implemented using blockchain technology, where all processes are recorded as transaction records inside the blockchain, and any kind of manipulation is strictly prohibited. The purpose of proposed approach is to identify the associated group by utilizing the direct management node of the ordinary node. The technique also aims to develop an authentication mechanism between these two entities. In order to meet the above-mentioned safety standards, it is essential that authentication techniques demonstrate resilience against commonly accepted standard security criteria.

Table 2. Simulation parameters.

Parameters	**Values**
Message size	0–500 MB
Environment Size	100 × 100
Node type	Cluster, ordinary and base station
Initial Energy of Each Node	0.5 Unit

The attacker will refrain from concealing the identification of another node in order to launch an attack, utilizing its distinct identity. In the context of an authenticated user, the initiation of authentication requests towards their cluster management nodes and the transmission of messages can exclusively be initiated by ordinary nodes upon entering the cluster network as shown in **Figure 5**. It provides comparisons between three types of nodes called cluster nodes, ordinary nodes, and base stations with respect to the size of messages during registration and authentication phases. The size of messages is reduced at the authentication phase because data compression techniques are used by blockchain networks to lower the overall size of messages during transmission. As a result, bandwidth utilisation can be optimised and latency decreased. The efficacy of this strategy should be evaluated by a comparative analysis with other schemes. Hence, commencing with the fundamental concept of the methodology, this study compares the computational utilization, storage utilization, and energy expenditure of diverse energy consumptions through the assessment of each stage in the execution procedure. **Figure 6** depicts the comparison of proposed mechanism in perspective of energy consumption. The comparison is performed by varying the computational capacity of nodes. The proposed mechanism achieves less energy consumption in perspective of existing technique i.e. AuBWSN (Authentication scheme using Blockchain for Wireless Sensor Networks)[25] because the existing approach uses Ethereum technology. The proposed framework uses local and global blockchain that will reduce energy consumption. In **Figure 7**, blocks of different sizes were examined to determine their corresponding objective values. The objective value depicts the efficiency of secure data monitoring using blockchain technology. In proposed mechanism objective value is less in perspective to AuBWSN technique because in proposed framework the public chain will retrieve from its initial base the unique identifiers for each participating node. When it comes to node authentication, the base stations have more storage space and keep track of public chain block information. In the IoT, nodes consume electricity largely during communication.

Figure 5. Comparison between cluster node, base station and ordinary nodes with respect to variation in message size in perspective of different phases.

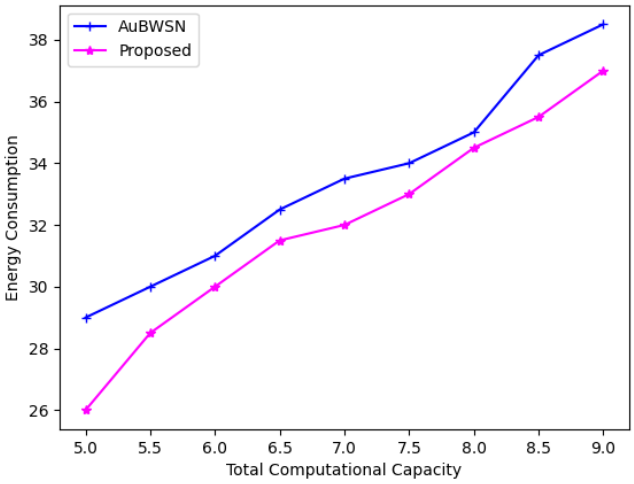

Figure 6. Comparison between SDTUB and AuBWSN in perspective of energy consumption.

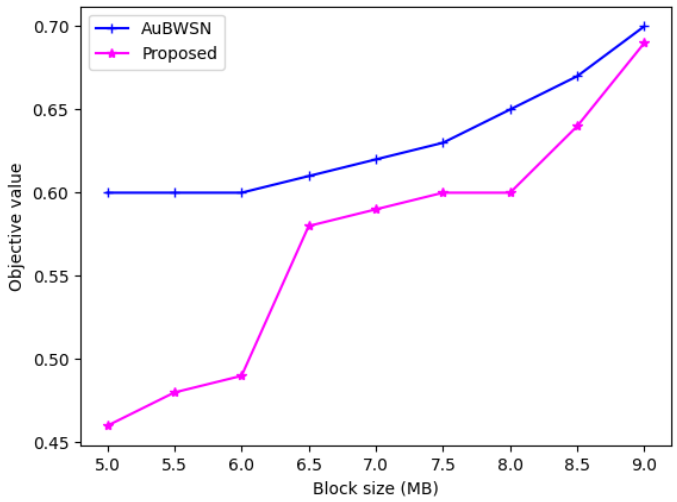

Figure 7. Comparison between SDTUB and AuBWSN techniques with respect to objective value.

6. Conclusion

This study introduces a unique methodology for augmenting data security in the Internet of Things (IoT) by employing a system based on blockchain technology. A customized blockchain architecture has been implemented to connect sensor networks among cluster administrators inside a singular IoT

system. Additionally, all IoT ground stations have been integrated into the public blockchain. The entire network is equipped with a hybrid blockchain paradigm. Significantly, the examination of safeguarding and outcomes demonstrates that the framework possesses a decent level of protection and productivity. Furthermore, the empirical findings demonstrate that the suggested system exhibits superior performance in relation to both security and computing efficiency. In a variety of scenarios, the simulation model demonstrates that the suggested technique has consistently outperformed other models in terms of response time and payload efficiency.

Author contributions

Conceptualization, SBB and SG; methodology, SBB and SG; software, MK; validation, SBB, SG and MK; investigation, SBB; resources, SG; data curation, MK; writing—original draft preparation, KS and RS; writing—review and editing, SBB, SC and KP; visualization, RE; supervision, NG; project administration, SBB and SG; funding acquisition, RE and NG. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Abosata N, Al-Rubaye S, Inalhan G, et al. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. Sensors. 2021, 21(11): 3654. doi: 10.3390/s21113654
2. Bezawada B, Bachani M, Peterson J, et al. Behavioral Fingerprinting of IoT Devices. Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security. Published online January 15, 2018. doi: 10.1145/3266444.3266452
3. Bai L, Yao L, Kanhere SS, et al. Automatic Device Classification from Network Traffic Streams of IoT. In Proceedings of the 2018 IEEE 43rd Conference on Local Computer Networks (LCN). IEEE. pp. 1-9. https://doi.org/10.1109/LCN.2018.8638098
4. Kolcun R, Popescu DA, Safronov V, et al. Revisiting IoT Device Identification. arXiv, 2018, arXiv:2107.07818.
5. Yousefnezhad N, Malhi A, Främling K. Automated IoT Device Identification Based on Full Packet Information Using Real-Time Network Traffic. Sensors. 2021, 21(8): 2660. doi: 10.3390/s21082660
6. Sabir A, Sheeraz A, Fasee U, et al. IoT with BlockChain: A Futuristic Approach in Agriculture and Food Supply Chain. Wireless Communications and Mobile Computing, 2021, 5580179. doi: 10.1155/2021/5580179
7. Yongxin L, Wang J, Li J, et al. ML for the Detection and Identification of IoT Devices: A Survey. IEEE Internet of Things Journal, 2020, 7, 298-320. doi: 10.1109/JIOT.2019.2922620
8. Azarmehr M, Mehta A, Rashidzadeh R. Wireless device identification using oscillator control voltage as RF fingerprint. In Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE. pp. 1-4. doi: 10.1109/CCECE.2017.7946629
9. Bihl TJ, Bauer KW, Temple MA. Feature Selection for RF Fingerprinting with Multiple Discriminant Analysis and Using ZigBee Device Emissions. IEEE Transactions on Information Forensics and Security. 2016, 11(8): 1862-1874. doi: 10.1109/tifs.2016.2561902
10. Wang C, Lin Y, Zhang Z. Research on Physical Layer Security of Cognitive Radio Network Based on RF-DNA. In Proceedings of the 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE. pp. 252-255. doi: 10.1109/QRS-C.2017.37
11. Zhang A, Zhang P, Wang H, Lin X. Application-oriented block generation for consortium blockchain-based IoT systems with dynamic device management. IEEE Internet of Things Journal, 2020, 8(10), 7874-7888. doi: 10.1109/JIOT.2020.3015042
12. Gong S, Tcydenova E, Jo J, et al. Blockchain-Based Secure Device Management Framework for an Internet of Things Network in a Smart City. Sustainability. 2019, 11(14): 3889. doi: 10.3390/su11143889
13. He Q, Xu Y, Liu Z, et al. A privacy-preserving Internet of Things device management scheme based on blockchain. International Journal of Distributed Sensor Networks. 2018, 14(11): 155014771880875. doi: 10.1177/1550147718808750

14. Wickstrom J, Westerlund M, Pulkkis G. Smart Contract based Distributed IoT Security: A Protocol for Autonomous Device Management. 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid). Published online May 2021. doi: 10.1109/ccgrid51090.2021.00094
15. Loukil F, Ghedira-Guegan C, Boukadi K, et al. Data Privacy Based on IoT Device Behavior Control Using Blockchain. ACM Transactions on Internet Technology. 2021, 21(1): 1-20. doi: 10.1145/3434776
16. Novo O. Scalable Access Management in IoT Using Blockchain: A Performance Evaluation. IEEE Internet of Things Journal. 2019, 6(3): 4694-4701. doi: 10.1109/jiot.2018.2879679
17. Moon H se, Song J, Shin H, et al. home IoT device management blockchain platform using smart contracts and a countermeasure against 51% attacks. 2022 4th Asia Pacific Information Technology Conference. Published online January 14, 2022. doi: 10.1145/3512353.3512381
18. Qureshi JN, Farooq MS, Abid A, et al. Blockchain applications for the Internet of Things: Systematic review and challenges. Microprocessors and Microsystems. 2022, 94: 104632. doi: 10.1016/j.micpro.2022.104632
19. Zhang K, Yu J, Lin C, et al. Blockchain-based access control for dynamic device management in microgrid. Peer-to-Peer Networking and Applications. 2022, 15(3): 1653-1668. doi: 10.1007/s12083-022-01316-5
20. Rana A, Sharma S, Nisar K, et al. The Rise of Blockchain Internet of Things (BIoT): Secured, Device-to-Device Architecture and Simulation Scenarios. Applied Sciences. 2022, 12(15): 7694. doi: 10.3390/app12157694
21. Li J, Herdem MS, Nathwani J, et al. Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management. Energy and AI. 2023, 11: 100208. doi: 10.1016/j.egyai.2022.100208
22. Rana SK, Rana SK, Nisar K, et al. Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare. Sustainability. 2022, 14(15): 9471. doi: 10.3390/su14159471
23. Deebak BD, Memon FH, Dev K, et al. TAB-SAPP: A Trust-Aware Blockchain-Based Seamless Authentication for Massive IoT-Enabled Industrial Applications. IEEE Transactions on Industrial Informatics. 2023, 19(1): 243-250. doi: 10.1109/tii.2022.3159164
24. Kairaldeen AR, Abdullah NF, Abu-Samah A, et al. Peer-to-Peer User Identity Verification Time Optimization in IoT Blockchain Network. Sensors. 2023, 23(4): 2106. doi: 10.3390/s23042106
25. Mubarakali A. An Efficient Authentication Scheme Using Blockchain Technology for Wireless Sensor Networks. Wireless Personal Communications. 2021, 127(1): 255-269. doi: 10.1007/s11277-021-08212-w