International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 4, August 2023, pp. 4422~4431
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i4.pp4422-4431

Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application

Martin Parmar, Parth Shah
Chandubhai S. Patel Institute of Technology, Faculty of Technology and Engineering, Charotar University of Science and Technology, Gujarat, India

Article Info

Article history:

Received Aug 22, 2022
Revised Jan 25, 2023
Accepted Feb 26, 2023

Keywords:

Data integrity
Data security
Internet of things synchronization
IoT-blockchain integration
Lightweight encryption

ABSTRACT

The industrial internet of things (IoT) plays a major role in the growth of automation and increasing digital connectivity for machine-to-machine communication. The research community has extensively investigated the possibility of IoT and blockchain integration for the last couple of years. The major research is focused on the benefits of integrating blockchain with IoT. In this work, we first focus on the issue of integrating IoT nodes with blockchain networks, especially for non-real-time IoT nodes that do not have an in-built clock mechanism. As a result, they cannot establish communication with real-time blockchain networks. Another critical security issue is protecting data coming from IoT devices to blockchain networks. Blockchain is enough mature to protect the data in its ecosystem. However, information coming from outside of the world does not have any guarantee of data integrity and security. This paper first addresses the clock synchronization issue of IoT nodes with blockchain using a network time protocol and then proposes an IoT-blockchain light-weight cryptographic (IBLWC) approach to secure the entire IoT-blockchain ecosystem. This paper also presents the performance analysis of IBLWC as a suitable and cost-effective solution that incurs less processing overhead for IoT-blockchain-based applications.

Corresponding Author:

Martin Parmar
Chandubhai S. Patel Institute of Technology, Faculty of Technology and Engineering, Charotar University of Science and Technology
Gujarat, India
Email: martinparmar.ce@charusat.ac.in

1. INTRODUCTION

By the end of 2025, there will be 30.9 billion connected devices, according to a statista.com study on the internet of things (IoT) devices and connections. According to this research, a volume of data needs to be processed and kept in a secure location. Hardware, software, and network configurations can vary widely in applications such as smart homes, smart cities, smart agriculture, and health care [1]. To process the data, each must deal with various sensors, IoT devices, gateways, and edge devices. IoT devices offer practical answers, such as less prone information that humans typically cause with poor intentions or errors [2]. To analyze the sensor data coming from legitimate IoT devices, it is imperative that its integrity, data security, and authenticity be preserved. In the context of intelligent IoT applications and associated problems, a few use cases are addressed below.

The fourth industrial revolution, known as the industrial IoT, allows machine-to-machine communication with little to no human involvement. Advanced analytics are used by industrial IoT to build industrial operations and act intelligently on collected data [3]. IoT devices will be connected by Ethernet and

Wi-Fi interfaces, creating a heterogeneous environment for this industrial ecosystem. To process the data in real-time, it develops into a very complex system and requires timely synchronization between all devices.

Figure 1 depicts an industrial setting where the various systems are heterogeneous [4]. While some devices connect via an Ethernet connection, others use a Wi-Fi interface. The entire communication is monitored and governed by a central administrator. The centralized gateway, which connects all the various devices, processes and stores the data at the edge gateway. Therefore, it has overhead for processing large amounts of data at the edge gateways. A data leak may occur if an unauthorized person gained access to the main system and altered the data. Therefore, the gateway device must be sufficiently secure to fend off such attacks. The processing load for processing the information is always increased by maintaining such procedures with high encryption at the edge devices. Another issue could develop because of the heterogeneity [5] in the environment, particularly with low-power devices that are not equipped with internal clocks and cause problems with time synchronization. This is especially true when the blockchain network is integrated because relies on real-time clock synchronization.

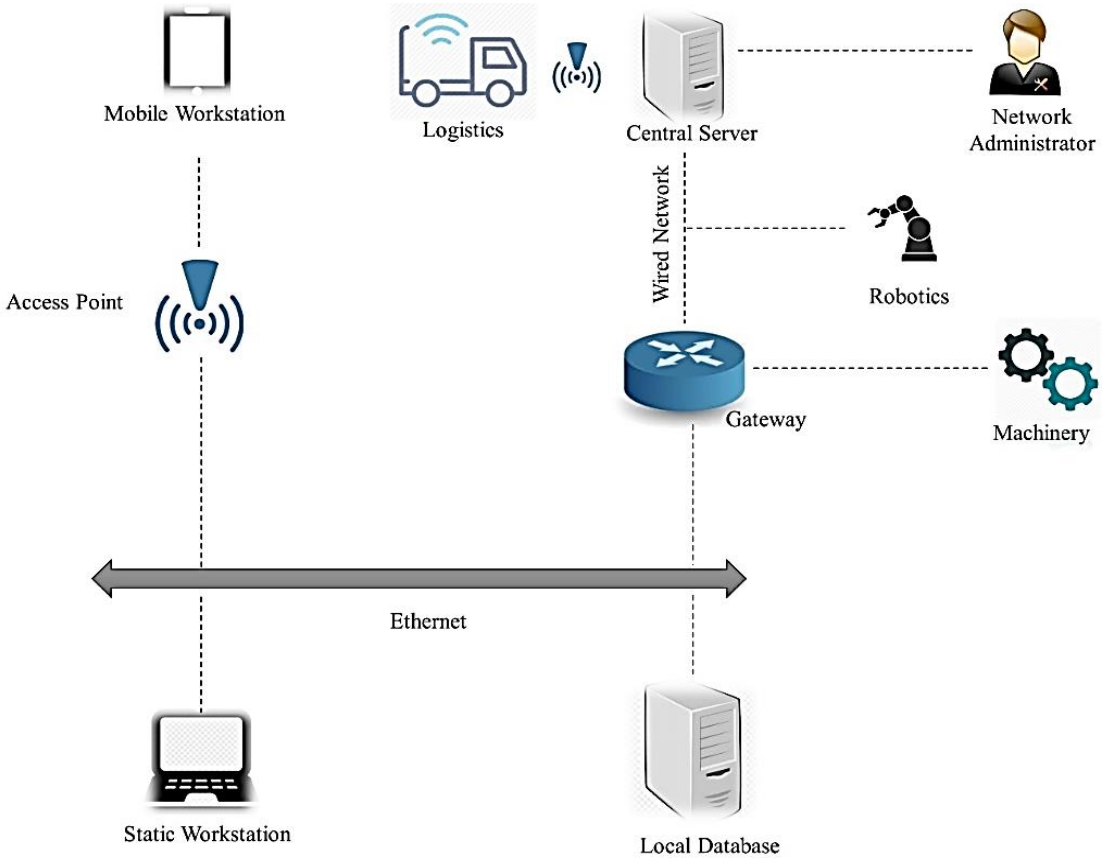

Figure 1. IoT industrial heterogeneous network system

With the least amount of human involvement, numerous tasks are carried out automatically in smart agriculture. For instance, by studying the weather that is best for farming, particularly concerning crops, and gathering data from sensors to examine farm fields, crops, water levers, sunlight, and pesticide usage [6]. Normally, all data are processed in a centralized system and saved locally or on external cloud storage. With the use of applications, this information can be used to forecast better crop management. Data integrity and security will therefore become key components of the ecosystem for smart agriculture. To prevent illegal access and alteration, the information must first be assembled through various sensor devices [7]. Second, the data must maintain its integrity at all costs after being verified and approved. For instance, while testing the quality of food coming from a farmyard, it should be prohibited to change any quality factors and to improve or downgrade the food's authenticity [8]–[10].

One of several domains that mainly comprises three primary functional categories is the medical domain: i) monitoring patient's health [11], ii) keeping patients' medical history data in central storage [12], and iii) medical drug supply chain. Health is tracked using various IoT and smart devices, including blood

pressure, temperature, oxygen levels, and activity tracking for fitness. The IoT sensor's incorporation into the medical field enables quick health evaluations and analysis of the information provided to forecast the outcome of any medical procedure or comprehend the cause of any sickness. Security and privacy are crucial and must be maintained at all costs to analyze patient data. IoT gazette generates much data, so it is necessary to send this data securely to the final storage location. Maintaining the patients' thorough medical history without compromising data integrity is the largest issue. The provision of medical drugs has also become a critical procedure that must offer openness, make it simple to track and trace drug information and stop any problems with drug counterfeiting [13], [14].

This study primarily focuses on IoT-Blockchain integration and emphasizes how to harness blockchain technology's potential to address the IoT infrastructure's problems. Blockchain technology is used in the study to protect the integrity of the data by storing it in the distributed ledgers of the participating peers [15]. However, data security becomes extremely important when data are sent to the blockchain network from external sources. When information is transmitted across an unsecured route, there must be a security check. Therefore, we need a security layer that shields against any attempted illegal access and alteration [16]. One potential scenario that could happen in these IoT-based blockchain applications is shown in Figure 2.

The following possible loopholes with the scenario presented in Figure 2: i) the attacker may access the node in case of a weak access control policy, especially for IoT devices; ii) the attacker may use a man-in-the-middle attack to intercept information by pretending to be a legitimate network; iii) the attacker may change any traffic data passing from the sensor source through communication channels; and iv) the attacker might launch a timing attack, especially on a low-powered node without an internal clock, cutting off communication with the remaining peers of the blockchain. In particular, on low-power IoT devices, this study focuses on data security by using a lightweight cryptographic technique to achieve data integrity and authentication.

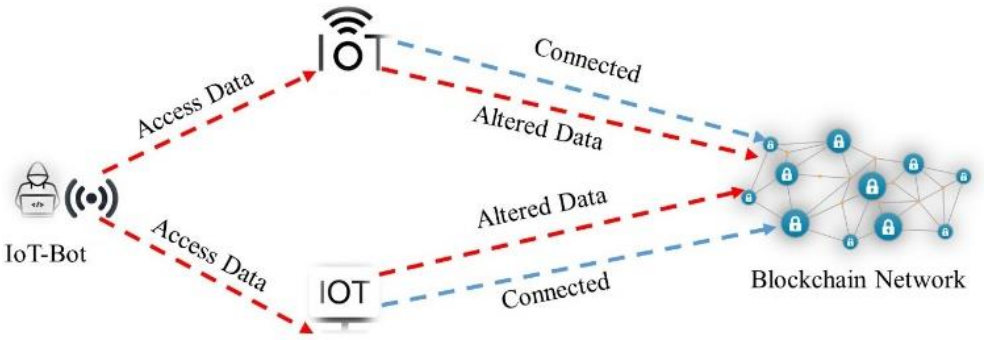

Figure 2. Data security issue in IoT-blockchain

2. RELATED WORK AND CONTRIBUTIONS

IoT challenges are covered in [17], particularly those involving heterogeneous networks and data processing that is centralized at the IoT-edge gateway. The concerns of centralized data processing and clock synchronization to non-real-time IoT nodes were raised by Misra *et al.* [17]. A distributed device-fingerprinting technique (DEFT) is presented in [18] and is used to identify IoT devices for applications like smart homes. The management and access control of IoT devices utilizing a decentralized blockchain are the main topics of [19], [20]. The author addressed the issue of the IoT smart system's centralized data processing, which results in overhead and other security concerns. The decentralized paradigm built on blockchain technology will offer precise access control along with scalable and transparent data monitoring. IoT and blockchain applications can be combined in the suggested solution.

A blockchain-based architecture for IoT-based applications was proposed in [21]. Access control and confidentiality are the main uses of attribute-based encryption (ABE), which the Rahulamathavan *et al.* [21] has put into practice. Another study examines the use of blockchain for IoT, particularly for applications related to smart cities. It outlines the difficulties in integrating blockchain and IoT as well as potential consensus mechanisms and platforms for putting any applications based on smart cities into use [22]. Sabireen and Neelanarayanan [23] give a certificate-based security solution among different layers such as IoT devices, edged devices, fog nodes, and cloud service providers. Moreover, it preserves the users' data privacy when information floats from one layer to another. Table 1 presents recent survey papers based on

IoT-Blockchain integration. The authors mention IoT issues and some challenges of integrating blockchain with IoT.

Table 1. IoT-blockchain survey

Reference	Year	IoT Issues	Challenges of Emergence Blockchain in IoT
[24]	2021	– Centralized processing Structure – Information may falsify during communication – Diversity of IoT based application with different framework raise the security problem	– IoT devices connectivity with blockchain – Power consumption and performance like throughput – Regularity issue and high cost
[25]	2018	– Confidentiality – Privacy – Data Integrity	– Keeping number of nodes live into the network – Increasing block size or decreasing block size – Scalability in terms of block size, response time and cost
[26]	2019	– Access control – information security – resource management	– Storage capacity and scalability – Legality – Consensus
[27]	2020	– Heterogeneity of IoT systems – Poor interoperability – Security vulnerability	– Extensive computing power for consensus and IoT devices are resource constraints – Big data analytics on large data – Scalability
[28]	2020	– Lack of guaranteed traceability and accountability – Inefficient handling of huge number of end-to-end communications – Data attack like unauthorized access and modification	– Designing security model for constrained IoT node and high-end blockchain node – Develop consensus like energy efficient for the low power IoT device
[29]	2020	– Data integrity – Data security – Robustness	– Scalability – Processing power – General rules and guidance for IoT blockchain integration
[30]	2021	– Data reliability – Authenticity – Maintenance	– Heterogeneity – Data security – Processing time
[31]	2021	– Centralization at fog computing – Privacy issue – Security attack	– High power consumption – Delay in response – Regulatory Issue
[32]	2018	– Data security – Data privacy	– Data privacy

Table 2. Cryptographic solution for IoT

Reference	Year	Issue Addressed	Solution
[32]	2018	Authentication	Two factor authentication using blockchain infrastructure
[33]	2019	Cryptographic encryption for IoT constrained devices	Lightweight message authentication for IoT devices
[34]	2020	Security for IoT devices	Blockchain based authentication protocol.
[35]	2021	Cloud data privacy	Blockchain based signature algorithm for cloud data privacy
[36]	2021	Access control for the centralized IoT system	Decentralized blockchain based access control for IoT system.
[37]	2021	IoT device's authenticity with security and privacy.	Blockchain based secure and lightweight authentication.
[38]	2021	Security, scalability, and identity access management	Blockchain based identity and access management for IoT devices.
[39]	2021	Water quality control and monitoring the factors to pollute the water.	IoT based water quality inspection and blockchain based penalty for polluting water.

The potential advantages of IoT and blockchain smart ecosystems, including smart cities, smart homes, health care, the industrial sector, and many others, have been heavily incorporated in a recent study. More research is needed on the emergence of blockchain technology with IoT for a smart ecosystem, as shown in Table 1. Particularly in IoT blockchain diverse situations, data integrity and authentication present significant issues. In blockchain, data immutability is only preserved and guaranteed until a strong consensus has been reached among peers or validators. However, it is crucial to protect data from unwanted modification or access when it comes from various IoT devices or sensors, particularly restricted IoT devices. We looked at research publications that discussed potential security solutions for IoT infrastructure security. In Table 2, the solutions also mention the crucial part that blockchain technology plays in IoT smart application development. The extensive research work presented by Patel and Shah [40] showcases the integration of IoT with different technologies and blockchain is one of them with issues of privacy, security, processing power, and time synchronization. In the next section, we configured a heterogeneous system with IoT and Ethereum as private blockchain networks.

2.1. Contributions

Both Node-1 and Node-2 have enough processing capacity to function as complete Ethereum blockchain nodes. The Raspberry Pi IoT devices Nodes-3 and Node-4 function as light nodes. Node-2 and Node-4 were connected via the Wi-Fi interface, while Node-1 and Node-3 were connected via Ethernet. A miner node that uses central processing unit (CPU) power is called Node 1. Additionally, Node-1 functions as a BootNode, which scans the network for other partner nodes. Peer nodes comprise the remaining nodes. We take into consideration the machine configuration shown in Table 3, the features of the Ethereum blockchain nodes shown in Table 4, and the blockchain node specification shown in Table 5. To build the Ethereum blockchain private network, all the requirements listed in Tables 3, 4, and 5 must be met. We have considered Node-1 from Table 4 as having two roles: one is the BootNode, which keeps track of all peer nodes, and the other is a miner node, which verifies the transaction in the blockchain network.

All the specifications needed to create the Ethereum blockchain network are listed in Table 5. The consensus process, gas limit, difficulty, and nonce parameters are specified in the *Genesis.json* file, which hardcoded the first genesis block and adds all future blocks in chronological order. The transaction's maximum energy expenditure is specified by the gas limit. The level of difficulty is set to low, medium, or high to control the rate of block formation. The goal reached by the miners to validate the transactions is a nonce, which is a number that is used just once. As a blockchain light node, we used two Raspberry PIs in this instance. The complete blockchain is synchronized and downloaded by the full node, which necessitates sufficient computing power and ongoing bandwidth support. A light node is limited to downloading the transaction receipt, making it simple to synchronize with another node, but it is unable to mine because that requires running as a full node. It is crucial to synchronize *time.nist.gov's* global clock with other blockchain-running nodes when using a Raspberry Pi as a full blockchain node. We've noticed that if the Raspberry Pi clock is behind the blockchain network, it will be unable to connect to other nodes. Since the Raspberry Pi lacks an internal clock as a personal computer does, it is important to set the clock each time [17]. Therefore, frequent disconnections from other blockchain peer nodes may be an outcome. As a result, the entire IoT-Blockchain ecosystem cannot be used for any real-time application that requires the processing and storing of sensor data. We set up a network time protocol (NTP) server to synchronize the clock regularly using the NTP. Instead of manually setting the clock, it will run service each time Raspberry starts up. The NTP server is set using the Ubuntu 18.0 platform, and the NTP clients are the Raspberry Pi.

Table 3. Machine configuration

Network-Size	Type	Network Type	Processor	RAM
Node-1	PC	Ethernet	Intel(R) Core (Tm) I5-8250u CPU @ 1.60 GHz	16.0 GB
Node-2	PC	Wi-Fi	Intel(R) Core (Tm) I5-8250u CPU @ 1.60 GHz	16.0 GB
Node-3	Raspberry Pi	Ethernet	Raspberry Pi 3 Model B+ Rev 1.3	1.0 GB
Node-4	Raspberry Pi	Wi-Fi	Raspberry Pi 3 Model B+ Rev 1.3	1.0 GB

Table 4. Ethereum blockchain node characteristics

Devices	Type	Sync. Mode	RPC/HTTP-Address	Node-Port	RPC/HTTP-Port
Node-1	BootNode & Miner	Full	172.16.3.209	30303	8545
Node-2	Peer	Full	172.16.3.221	30310	8546
Node-3	Peer	Light	172.16.3.204	30311	8547
Node-4	Peer	Light	172.16.101.124	30312	8548

Table 5. Ethereum blockchain node specification

Features	Type
Platform	Ethereum 1.0
Client	Go-Ethereum (Geth) 1.9
Consensus Mechanism	POA
Block-Size	Default (1 Mb)
Gas-Limit	16777216
Difficulty	0x100000
Nonce	66

3. SYSTEM ARCHITECTURE AND PROPOSED WORK

Figure 3 represents a heterogeneous IoT-Blockchain integrated network system. All the peer nodes synchronize using the NTP server. We have mentioned one NTP server, but it is also possible to set up a cluster of servers responsible for the standard time synchronization, especially with the IoT-constrained node.

All the nodes, such as IoT and blockchain connected using the exact NTP time synchronization. Specifically, for IoT-constrained devices, the following code will run as a service on the booting time of the constrained IoT device. This will synchronize the NTP time clock to the constrained IoT devices automatically.

```
while SNTP ON      do
     check and verify SNTP (dt)
     CNTP STOP
     if (dtNTP==SNTP) then
        CNTP START
     end if
end while
```

The blockchain node regularly coordinates, so NTP becomes crucial to synchronize the clock timing. The same is possible with IoT constrained devices that coordinate with blockchain nodes.

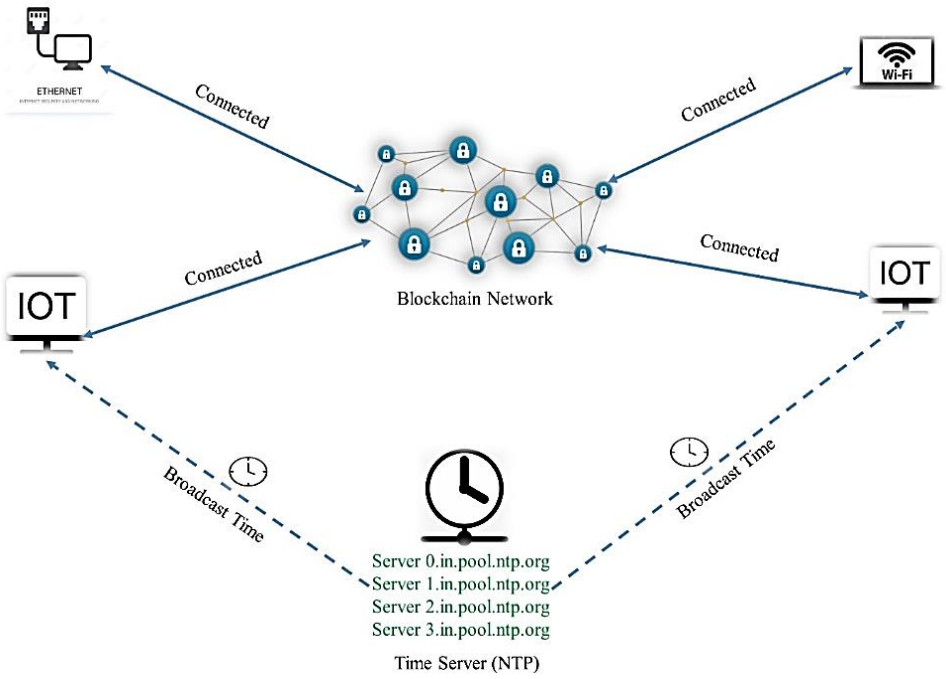

Figure 3. Synchronized IoT-blockchain heterogeneous network

3.1. IoT-blockchain-light-weight cryptography proposed approach

Our proposed approach is to apply IoT-blockchain light-weight cryptography (IBLWC) to prevent data attacks. The proposed approach steps are given below.

- The IoT node senses the data and performs hashing using the SHA256 algorithm.
- Hashing applies over an original message (*m*) and secret code (*s*). The secret code is an Enode-ID of BootNode:
  enode://16d01ad8e1c94f4c385d8c4693fe22d80bc84c4909184fd9bbc5ce227241856d04c83966a4652b5f0ef6e8e3687e4d6da9857f0912101c4d6a3fd7a4cc06d3b4@172.16.3.209:30303
- Computed hash code (*h'*) along with original message (*m*) send to blockchain network.
- Blockchain nodes can easily verify the legitimate node from the peer list.
- Receiving node calculates hash from received original message (*m'*) and secret code (*s*) as Enode_ID of BootNode.
- Finally, the node can verify calculated hash code (h) with received hash code (h').
- If both the hash codes match, the data will be accepted, or it will be rejected in case of hash mismatch.

The proposed approach mentioned in Figure 4 presents message integrity and authentication. This scenario is applicable when no more secrecy is required. The recipient node can authenticate the communicating node with a unique secret code. This lightweight approach avoids the process of heavy encryption. The proposed work identifies the communicating node as a legitimate node through authentication using a secret code and preserves data integrity.

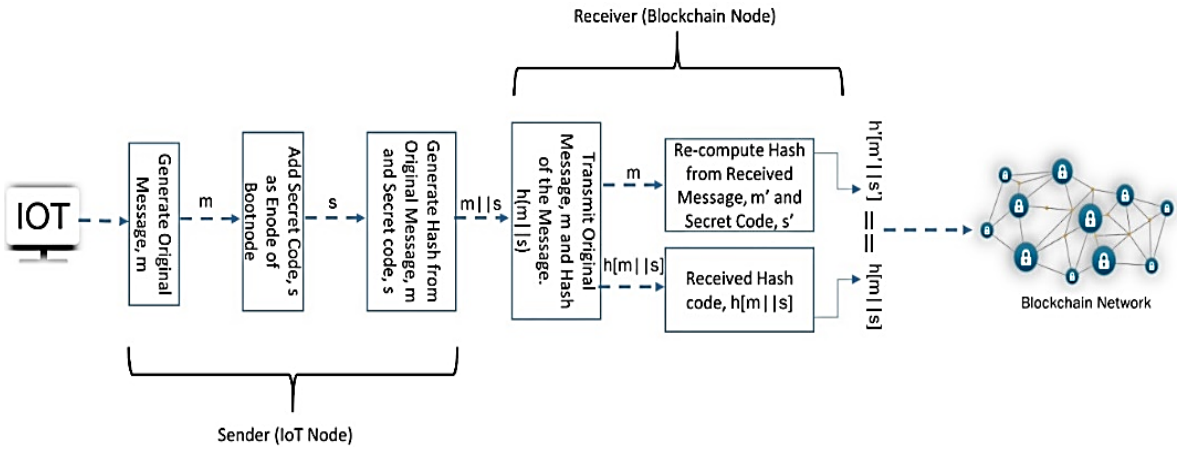

Figure 4. Proposed approach with message authentication and message integrity

The proposed approach preservers the single preimage resistance from (1) where the attacker cannot get the original message (*m*) from (2) and (3).

$$m = h(m) \tag{1}$$

$$\text{Attacker} -> h(m) = m' \tag{2}$$

$$m \neq m' \tag{3}$$

The proposed approach preserves the second preimage resistant from (4) which is a unique hash of the input message.

$$m = h(m) \tag{4}$$

The attacker has the original message and hash of the message. The attacker tries to create the same hash of two different messages from (5).

$$h(m') == h(m) \text{ where } m \neq m' \tag{5}$$

The proposed approach also preserves the collision resistance where the attacker cannot form pair from (6).

$$(m1, m2) => h(m1), h(m2) \text{ where } h(m1) == h(m2) \text{ and } m1 \neq m2 \tag{6}$$

The proposed approach prevents any unauthorized data access and unauthorized data alternation. Moreover, this approach will not require much computing overhead as no such process-heavy encryption is used. The following section contains the performance measurement of the above-mentioned proposed approach in terms of average latency, CPU computing power with mining, and CPU overhead after applying the proposed approach to the entire IoT-Blockchain ecosystem.

3.2. Performance matrix and performance evaluation

We used the Go Ethereum Client (Geth 1.9) to set up the blockchain network, as discussed in section 2. The data is stored in the individual node's local storage, a distributed ledger. Table 6 presents the read and write transactions respective to latency and throughput.

The latency specifically for write transactions is mainly dependent on mining the transaction. For example, bitcoin takes approximately 10 min to mine one block of transaction and Ethereum 1.0 supports approximately 12 to 14 seconds to mine a new block. Blocktime refers to the time required to produce the next block, and block size defines the total capacity to store transactions in one block. The current size of the block is 1 MB. We did performance testing of our IoT-blockchain ecosystem using Etherscan API. We analyzed the average latency of the network, and computing power of the CPU with our proposed work in the following result analysis section.

Table 6. Evaluation parameters of blockchain network [41]

Latency	Read	The time when sending read request and get the response.
	Write	A time when the transaction sends and time to wait for a network-wide transaction to perform.
Throughput	Read	The total number of reading requests per defined time.
	Write	A total number of valid transactions performs in a defined time over the network.

3.3. Result analysis

It was observed from Figure 5(a) that Node-4 (Raspberry Pi) has high latency compared to other nodes. Node-4 connected using the Wi-Fi interface caused some network delay compared to the node connected using the Ethernet interface. All the nodes are connected using standard organization internet to maintain proper clock synchronization of constrained IoT nodes with blockchain nodes. We observe the critical CPU usage in a constrained and non-constrained node in Figure 5(b). Node-1 and Node-2 are full computing nodes with minimum CPU load after mining operations. Node-4 has a high CPU load after mining, as it is a constrained node. Node-3 is also a constrained node, but it has lower CPU usage than Node-4 with a Wi-Fi interface. The common observation is that the CPU usage of constrained devices is under 50% after doing some mining work. The CPU usage can be minimized by considering the Raspberry Pi node as a light Ethereum node. A light node cannot be part of any mining work, so there will be no computational overhead except for cryptographic operations.

Finally, we applied our proposed approach to secure every communication from IoT to blockchain and analyze computing power, especially on constrained devices. Figure 5(c) shows the low CPU overhead using the proposed approach IBLWC compared to processing heavy encryption using Rivest-Shamir-Adleman (RSA) and advanced encryption standard (AES) on IoT constrain nodes. Our approach is based on message integrity and message authentication using a secret code as BootNode's Enode-ID. BootNode provides an easy way to identify the legitimate participating node in the blockchain network. Thus, BootNode gives a handy access control mechanism. Our approach gives significant performance between IoT and blockchain networks to protect data.

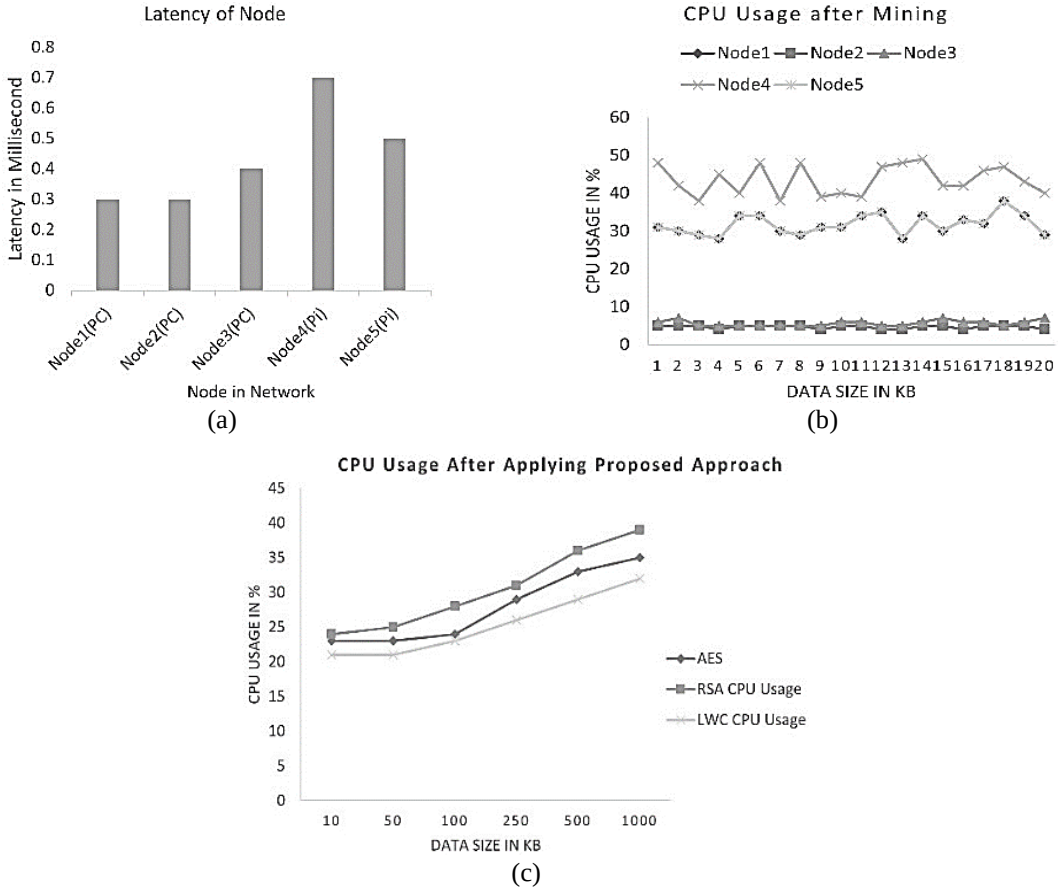

Figure 5. Result analysis of (a) average latency of node, (b) CPU usage after mining (c) CPU usage after applying proposed approach

4. CONCLUSION

The integration of IoT and blockchain has significant advantages like atomization and intelligent features. However, it is essential to handle time synchronization for constrained IoT nodes before integrating with the blockchain network. To do that, we formed a heterogeneous IoT-blockchain system with constrained and non-constrained nodes such as Raspberry Pi and a personal computer with sufficient computing power. We used the existing NTP-based solution to synchronize the clock of constrained IoT nodes that do not have a built-in clock mechanism. Thus, the constrained IoT node can connect with the blockchain network easily. This low-cost set scenario of an IoT-blockchain system can be applicable at the initial stage to check the feasibility and other complexity of any IoT-blockchain-based intelligent applications. We observed the critical problem of data security breaches, especially at constrained sensor nodes that capture the traffic and alter the sensor value. To prevent this, we proposed the IBLWC approach. The performance analysis shows that the average CPU usage and average latency are minimum during mining operations after applying the proposed approach. It can also minimize by increasing the number of miners' nodes in the blockchain network to do more parallel work to validate the transactions.

REFERENCES

[1] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *Journal of Network and Computer Applications*, vol. 181, May 2021, doi: 10.1016/j.jnca.2021.103007.

[2] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: challenges and solutions," *Applied Sciences*, vol. 10, no. 12, Jun. 2020, doi: 10.3390/app10124102.

[3] G. Li *et al.*, "GT-chain: a fair blockchain for intelligent industrial IoT applications," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3244–3257, Sep. 2022, doi: 10.1109/TNSE.2021.3099953.

[4] T. Kim, C. Ramos, and S. Mohammed, "Smart city and IoT," *Future Generation Computer Systems*, vol. 76, pp. 159–162, Nov. 2017, doi: 10.1016/j.future.2017.03.034.

[5] Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in internet of things: a survey," *SN Applied Sciences*, vol. 3, no. 1, Jan. 2021, doi: 10.1007/s42452-021-04156-9.

[6] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldύ, "The rise of blockchain technology in agriculture and food supply chains," *Trends in Food Science and Technology*, vol. 91, pp. 640–652, Sep. 2019, doi: 10.1016/j.tifs.2019.07.034.

[7] G. da S. R. Rocha, L. de Oliveira, and E. Talamini, "Blockchain applications in agribusiness: a systematic review," *Future Internet*, vol. 13, no. 4, Apr. 2021, doi: 10.3390/fi13040095.

[8] M. H. Ronaghi, "A blockchain maturity model in agricultural supply chain," *Information Processing in Agriculture*, vol. 8, no. 3, pp. 398–408, Sep. 2021, doi: 10.1016/j.inpa.2020.10.004.

[9] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on security threats in agricultural IoT and smart farming," *Sensors*, vol. 20, no. 22, Nov. 2020, doi: 10.3390/s20226458.

[10] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A survey on the role of IoT in agriculture for the implementation of smart farming," *IEEE Access*, vol. 7, pp. 156237–156271, 2019, doi: 10.1109/ACCESS.2019.2949703.

[11] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: a systematic review," *Healthcare*, vol. 7, no. 2, Apr. 2019, doi: 10.3390/healthcare7020056.

[12] M. A. Tunc, E. Gures, and I. Shayea, "A survey on IoT smart healthcare: emerging technologies, applications, challenges, and future trends," *arXiv preprint arXiv:2109.02042*, Sep. 2021.

[13] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[14] L. M. Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," *Electronics*, vol. 8, no. 7, Jul. 2019, doi: 10.3390/electronics8070768.

[15] O. Novo, "Blockchain meets IoT: an architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: 10.1109/JIOT.2018.2812239.

[16] F. H. Pohrmen, R. K. Das, and G. Saha, "Blockchain-based security aspects in heterogeneous Internet-of-Things networks: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 10, Oct. 2019, doi: 10.1002/ett.3741.

[17] S. Misra, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, and M. Rajarajan, "Blockchain at the edge: performance of resource-constrained IoT networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 1, pp. 174–183, Jan. 2021, doi: 10.1109/TPDS.2020.3013892.

[18] V. Thangavelu, D. M. Divakaran, R. Sairam, S. S. Bhunia, and M. Gurusamy, "DEFT: a distributed IoT fingerprinting technique," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 940–952, Feb. 2019, doi: 10.1109/JIOT.2018.2865604.

[19] A. Ouaddah, "A blockchain based access control framework for the security and privacy of IoT with strong anonymity unlinkability and intractability guarantees," in *Advances in Computers*, Elsevier, 2019, pp. 211–258.

[20] S. Pal, A. Dorri, and R. Jurdak, "Blockchain for IoT access control: Recent trends and future research directions," *Journal of Network and Computer Applications*, vol. 203, Jul. 2022, doi: 10.1016/j.jnca.2022.103371.

[21] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Dec. 2017, pp. 1–6, doi: 10.1109/ANTS.2017.8384164.

[22] A. Rejeb, K. Rejeb, S. J. Simske, and J. G. Keogh, "Blockchain technology in the smart city: a bibliometric review," *Quality and Quantity*, vol. 56, no. 5, pp. 2875–2906, Oct. 2022, doi: 10.1007/s11135-021-01251-2.

[23] H. Sabireen and V. Neelanarayanan, "A review on fog computing: architecture, fog with IoT, algorithms and research challenges," *ICT Express*, vol. 7, no. 2, pp. 162–176, Jun. 2021, doi: 10.1016/j.icte.2021.05.004.

[24] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54478–54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[25] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: a systematic survey," *Sensors*, vol. 18, no. 8, Aug. 2018, doi: 10.3390/s18082575.

[26] D. A. Noby and A. Khattab, "A survey of blockchain applications in IoT systems," in *2019 14th International Conference on Computer Engineering and Systems (ICCES)*, Dec. 2019, pp. 83–87, doi: 10.1109/ICCES48960.2019.9068170.
[27] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.
[28] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.
[29] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems," *ACM Computing Surveys*, vol. 53, no. 1, pp. 1–32, Jan. 2021, doi: 10.1145/3372136.
[30] M. N. M. Bhutta *et al.*, "A survey on blockchain technology: evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.
[31] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: challenges and solutions," *Blockchain: Research and Applications*, vol. 2, no. 2, Jun. 2021, doi: 10.1016/j.bcra.2021.100006.
[32] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, Mar. 2018, pp. 769–773, doi: 10.1109/ICCNC.2018.8390280.
[33] G. Saldamli, L. Ertaul, and A. Shankaralingappa, "Analysis of lightweight message authentication codes for IoT environments," in *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, Jun. 2019, pp. 235–240, doi: 10.1109/FMEC.2019.8795359.
[34] M. Yavari, M. Safkhani, S. Kumari, S. Kumar, and C.-M. Chen, "An improved blockchain-based authentication protocol for IoT network management," *Security and Communication Networks*, pp. 1–16, Oct. 2020, doi: 10.1155/2020/8836214.
[35] G. Xie, Y. Liu, G. Xin, and Q. Yang, "Blockchain-based cloud data integrity verification scheme with high efficiency," *Security and Communication Networks*, pp. 1–15, Apr. 2021, doi: 10.1155/2021/9921209.
[36] S. Algarni *et al.*, "Blockchain-based secured access control in an IoT system," *Applied Sciences*, vol. 11, no. 4, Feb. 2021, doi: 10.3390/app11041772.
[37] X. Yang *et al.*, "Blockchain-based secure and lightweight authentication for internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3321–3332, Mar. 2022, doi: 10.1109/JIOT.2021.3098007.
[38] R. Fotohi and F. Shams Aliee, "Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT," *Computer Networks*, vol. 197, Oct. 2021, doi: 10.1016/j.comnet.2021.108331.
[39] N. Alharbi, A. Althagafi, O. Alshomrani, A. Almotiry, and S. Alhazmi, "A blockchain based secure IoT solution for water quality management," in *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, Jul. 2021, pp. 1–8, doi: 10.1109/ICOTEN52080.2021.9493474.
[40] B. Patel and P. Shah, "Operating system support, protocol stack with key concerns and testbed facilities for IoT: A case study perspective," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5420–5434, Sep. 2022, doi: 10.1016/j.jksuci.2021.01.002.
[41] M. Parmar and P. Shah, "Uplifting blockchain technology for data provenance in supply chain," *International Journal of Advanced Science and Technology*, vol. 29, pp. 5922–5938, 2020.

BIOGRAPHIES OF AUTHORS

Martin Parmar is a Ph.D. student in the field of computer engineering at Charotar University of Science and Technology (CHARUSAT), Anand, Gujarat, India. He received his master's degree in the field of computer science and engineering from Gujarat Technological University (GTU) in 2014. His major area of research includes information security, blockchain, and cryptocurrency. He can be contacted at martinparmar.ce@charusat.ac.in.

Parth Shah obtained his Ph.D. degree in the area of cloud computing from CHARUSAT, Gujarat, India in 2017 and a master's degree in computer engineering in 2004, Gujarat, India. He is a professor at the Department of Information Technology, Charotar University of Science and Technology (CHARUSAT), Anand, Gujarat, India. His research interest includes parallel computing, next-generation networks, advanced computer architecture, and cloud computing. He can be contacted at parthshah.ce@charusat.ac.in.