Internet of things-blockchain integration: a robust data security approach for end-to-end communication

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

Article Info

Article history:

Received Apr 19, 2023
Revised Jul 27, 2023
Accepted Aug 7, 2023

Keywords:

Authentication
Data integrity
Data security
IoT security
IoT-blockchain integration

ABSTRACT

The integration of internet of things (IoT) and blockchain technology has been proposed as a promising solution to address the challenges related to security, scalability, and privacy. This integration enables the creation of secure and decentralized systems that allow devices to interact with each other and exchange data in a transparent and trustworthy manner. The significant research work has been carried out by researcher on IoT and blockchain integration to utilize their combine potential in smart applications. However, due to limitation and scope of emerging technologies, it is essential to develop robust security frameworks that address the challenges and ensure the secure data communication from IoT node to blockchain network. IoT devices come up with constrained nature and limited security mechanisms along with weak access control policy. Our work includes heterogeneous IoT and blockchain ecosystem that senses and store data intelligently after proper validation with verification into decentralized distributed blockchain network. Our proposed work includes a robust approach to convey potential data security issue to protect end to end information with suitable authorization, access control policy, device to device data protection and data integrity specially when data moving from IoT devices to blockchain network.

Corresponding Author:

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

1. INTRODUCTION

Internet of things (IoT) is a technology that enables the interconnectivity of physical devices, data collection, analysis, and sharing of information [1]. The integration of the IoT and blockchain technology has enormous potential to revolutionize several industries, including smart agriculture, food supply chain management, and industrial internet of things (IIoT). This integration can bring increased efficiency, transparency, and security to these industries [2]. This technology can help farmers optimize their use of resources, reduce waste, and increase yields. IoT can be used in livestock farming to watch over animal health, keep track of where the animals are, and control when they eat and drink [3].

In the food supply industry, IoT is used to make distributing and storing food products better [4]. IoT sensors keep an eye on the temperature and humidity in places where food is stored or transported. This helps make sure that the food stays fresh and safe to eat. However, there are many problems and difficulties with using IoT in areas like farming, healthcare, and industries. Here are the main problems to pay attention to.

- Connectivity [5]: IoT devices need a strong and dependable network to send information. In countryside areas, where farming is common, the network might not be powerful enough to handle many IoT devices being used.
- Data security and privacy [6]: IoT devices produce lots of important information that needs to be safeguarded from online dangers. Farmers and those involved in the food supply chain must make sure that their IoT systems have proper security measures to keep their data and privacy safe.
- Data interoperability [7]: Various IoT devices and systems may use different rules and guidelines, which can make it difficult to connect them together into one system.

Research has been made on how blockchain can be used to keep a safe and clear device data and transactions. The information can be saved on a blockchain, creating a safe and unchangeable record of all machine transactions. Here are some advantages of merging blockchain technology with IoT.

- Security: Internet of things devices can be easily attacked by hackers, but Blockchain technology offers strong protection because it is decentralized. This means it is hard for hackers to change or manipulate the data.
- Data integrity: IoT devices create lots of data, and blockchain technology makes sure this data is reliable by keeping a secure and open record of all actions that can't be changed.
- Decentralization: IoT devices can talk to each other without needing a central person or system to control them. Blockchain helps with managing data in a decentralized way, which makes it safe and trustworthy for devices to communicate with each other [8].
- Efficiency: Blockchain technology makes transactions faster and cheaper for IoT by getting rid of middlemen.

Combining IoT and blockchain can change how we connect with the digital world by making it safer, faster, and more dependable for devices to talk to each other [9]. However, connecting the IoT with blockchain technology comes with many research and technical difficulties. First, it is very important to make sure that data is accurate and secure.

2. RELATED WORK IN IOT-BLOCKCHAIN INTEGRATION

Blockchain is a type of technology that keeps track of information digitally. It is not controlled by just one person or organization [10]. Technology is like a digital filing system that keeps information safe and visible to everyone. It uses secret codes to make sure the data is real and trustworthy. It also needs many people to agree on the information before it gets added to the blockchain. One important thing about blockchain is that once data is added to it, it can't be changed or removed. This makes it a perfect platform for keeping track of transactions because it gives a secure and clear record of all transactions that have taken place on the network [11]. A blockchain is like a big digital spreadsheet that keeps track of lots of information and is shared among many different people [12]. Each piece of information is stored in blocks, and new blocks keep getting added to the list as more information is added. Each group has a bunch of transactions and an important information about the group. The block header is an 80-byte structure that has different parts:

- Version: This field specifies the version of the block.
- Previous block hash: This field contains the 32-byte hash of the previous block in the blockchain.
- Merkle root hash: This field contains the 32-byte hash of the Merkle root of all the transactions in the block.
- Timestamp: This field specifies the time when the block was created.
- Difficulty target: This field specifies the difficulty level required for a block to be considered valid.
- Nonce: This field is a 32-bit integer that is used in the process of mining to generate a hash that meets the difficulty target.

The Merkle root hash is found by combining the hashes of all the transactions in the block. This is done by taking pairs of transaction hashes and finding the hash of each pair. The process is repeated until only one hash is left. This special hash is put in the block's header. The header of the block, along with the transactions in the block, is combined and transformed using a special security function called secure hash algorithm (SHA256). This creates a 32-character code called the block hash. The block hash is what makes each block special, and it is used to connect blocks and make a chain. The previous block hash field in the block header is used to connect each block to the block that came before it in the chain.

Blockchain consensus protocols are really important for blockchain technology. They help a bunch of computers agree on what transactions are valid and make sure the blockchain stays secure [13]. Multiple agreement plans have been developed over the years, each with their own set of advantages and disadvantages. Here are some of the most well-liked consensus protocols and their features:

- Proof of work (PoW) is the initial protocol used in the Bitcoin that is first application of blockchain. PoW is known for being very secure, but it uses a lot of energy to solve cryptographically mathematical puzzle using computational power. This leads to higher fees for transactions and longer processing times [14].
- Proof of stake (PoS) is a different way to reach an agreement, compared to PoW. Instead of solving math problems, PoS asks validators to put away some cryptocurrency to join the network and check transactions. PoS requires less energy than PoW, which means transaction fees are cheaper and processing speeds are faster [14].
- Delegated proof of stake (DPoS) is a type of PoS where people can vote for delegates who will verify transactions and add new blocks to the blockchain. DPoS is faster than PoS because it uses a smaller group of validators, but it is also more centralized because only a few delegates control the network [14].
- Proof of authority (PoA) is a way to agree on transactions and add them to the blockchain by using a specific number of validators. Validators are chosen because they are well-known and trusted, and they must have a specific amount of ownership in the system. PoA is a fast and efficient system [14].

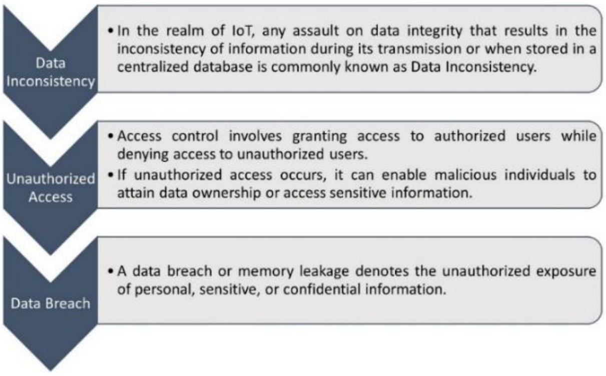
Our work is mainly focus to address data security issue presented by author in Figure 1 [15]. IoT energy constrain devices are often vulnerable to cyber-attacks, so integrating them with blockchain technology requires a robust security framework. It is necessary to authenticate legitimate IoT node, protect the information communicated from legitimate node to blockchain node and also data integrity of IoT node. Access control implies giving access to authorized users and blocking access to unauthorized users. Data breach refers to the disclosure of personal, sensitive, or confidential data in an unauthorized manner.

The majority work presented in the Table 1 are focused on IoT issues and its solution using blockchain technology [16]–[25]. IoT and blockchain integration has heterogeneous complex system including some constrained IoT node as well as full computing node. The security, authentication, access control and data integrity always crucial between IoT node to blockchain network.

Our work presented in [26] was based on time synchronization of constrain IoT node with blockchain real time network. We focused the data integrity issue using lightweight cryptographic approach by appending secret code of bootnode. This work is an extension of our previous work that addresses overall data security issues using encryption and secret code of individual IoT node. Next session is based on our extended proposed work for IoT-blockchain system.

Table 1. Related work in IoT and blockchain integration

Research Paper	Issues	Proposed Solutions	Application
[16]	Complex supplychain system to track and trace agriculture food.	To provide traceability in agriculture supplychain with user centric approach using permissioned Blockchain network.	Agriculture
[17]	Lack of data accessibility and data management across global supplychain	To provide study report on Blockchain technology used for agriculture supplychain during COVID-19.	Industrial agriculture product COVID-19
[18]	Technical challenges such as interoperability among different Blockchain and Security concern with IoT to detect counterfeiting.	Give the details view of various areas where Blockchain can be used and provide research challenges using Blockchain.	Supplychain
[19]	Unauthorized access to confidential data of agriculture. Unmanaged data and not easily trace information.	IoT-Edged and Blockchain based solution to provide security, privacy and information tracing to take smart decision to increase crop productivity.	Agriculture
[20]	IoT security issue for authentication as legitimate devices.	Provide security layer between fog node and user to communicate information.	Face recognition
[21]	Centralized security issue of IoT having single point of failure. Computation overhead of Blockchain node	Provide cluster-based solution of IoT nodes to reduce computation overhead.	IoT-blockchain network
[22]	Blockchain privacy issue and vulnerability in Smartcontract code.	Details study on Blockchain confidentiality and privacy preserving scheme.	IoT-blockchain
[23]	Difficulty to produce, process and store evidence of forensics record due to heterogeneity of IoT devices.	Provide decentralized Blockchain solution to manage forensics records.	Blockchain-IoT forensics
[24]	Different platforms to process data, unknown participants to make system trustless and stakeholder communication.	Proposed Agri-Food IoT based framework to provide decentralized trusted platform for Agriculture Food supplychain.	IoT-blockchain Food supply chain
[25]	Food loss, food safety and food security.	Provide detail study on Blockchain based solution for transparent and traceable system.	Agriculture food sector



Data Inconsistency
- In the realm of IoT, any assault on data integrity that results in the inconsistency of information during its transmission or when stored in a centralized database is commonly known as Data Inconsistency.

Unauthorized Access
- Access control involves granting access to authorized users while denying access to unauthorized users.
- If unauthorized access occurs, it can enable malicious individuals to attain data ownership or access sensitive information.

Data Breach
- A data breach or memory leakage denotes the unauthorized exposure of personal, sensitive, or confidential information.

Figure 1. Data attack on IoT [15]

3. PROPOSED METHOD

Our proposed model is based on the architecture presented in Figure 2. The internet of things (IoT) and blockchain ecosystem has three layers which are application layer at upper to provide user access to blockchain network. The second is the IoT layer at bottom that has IoT devices with sensors to capture data, to process the data as well as to transfer into blockchain network through gateway. The third is the proposed security layer to protects information communicated between application layer and gateway as well as from IoT devices to gateway. The security layer ensures privacy that only the desired sensor devices and gateways are part of the network. The security layer ensures authenticity that the supposed sender is the real sender. The security layer ensures confidentiality that the data is only readable by the proposed destination. Finally, the security layer ensures integrity that the information contained in the original message is kept intact.

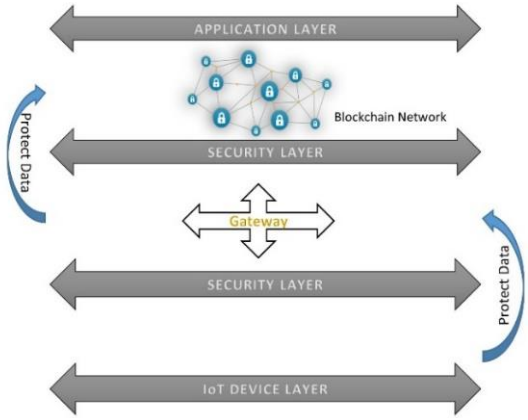


Figure 2. IoT and blockchain conceptual architecture

The proposed approach has the following main steps:

a. Each device generates the secret code which is unique in communicating with end device.
b. The controller (server) maintains the list of characteristics such as enode, RPC/HTTP_Address, RPC/HTTP_Port and secret keys for each node.
c. IoT device appends the secret code with original message and produce hash code using secure hash algorithm (SHA256) hashing algorithm. The secret code is its own enode id.
d. IoT device applies encryption using symmetric key, advanced encryption standard (AES) algorithm over calculated hash and original message.
e. IoT controller device preforms the decryption by applying the same secret key shared between legitimate IoT device and controller.
f. IoT controller computes the hash using SHA256 from received original message and the same secret code that is used by intended IoT device.
g. IoT controller verifies message integrity and message authentication as well as identify any legitimate node from the properties list. The list keeps updating dynamically whenever it requires.

h. To process data into blockchain network, IoT controller computes hash from data and its Enode id.
i. Controller performs encryption using its private key to sign digitally signs over computed hash and original data. This ensure strong authentication from legitimate device.
j. Finally, the blockchain network specifically validator node will do decryption using public key and verify the message content and original sender.

The overall proposed approach is presented in Figure 3 along with encryption algorithm and hashing algorithm. The IoT controller acts as bootnode of Blockchain. The bootnode keeps monitoring on all the participant nodes into the network. The bootnode can capture all the enode id of individual node and verify whether it is legitimate node or not.

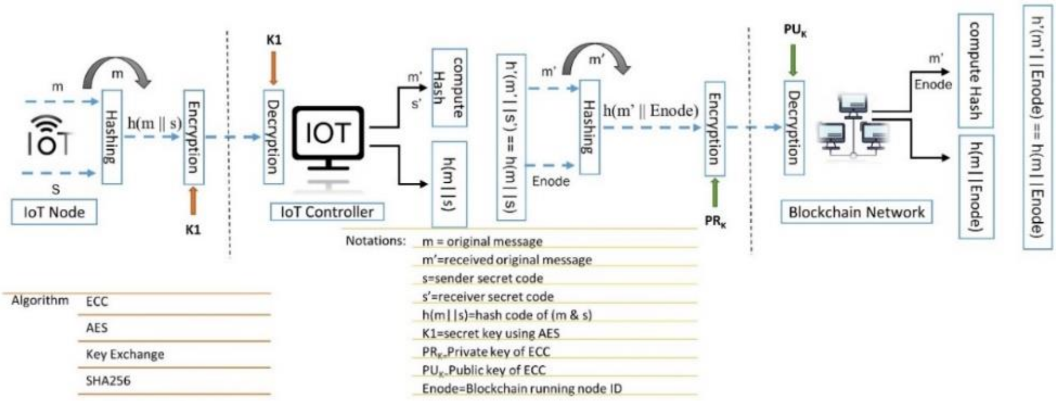


Figure 3. Overall process flow of proposed approach

Any IoT node that wants to communicate with IoT controller, it required to use its enode id as secret code. The enode id is unique identity of running blockchian node. Thus, bootnode can automatically discover any peers into the network and use the same enode id to verify the content integrity. Following are mathematical representation of various operations such as encryption, decryption and hashing at IoT sender, IoT controller and blockchain network.

IoT node to IoT controller node:

Hashing: $x = H(m, s)$ (1)

Encryption: $E(K1[x, m])$ (2)

Decryption: $D(K1[x, m])$ (3)

Verification: $x' = H(m, s)$, x == x' (4)

IoT controller to Blockchain network:

Hashing: $y = H(m', Enode)$ (5)

Encryption: $E(PRkey[m', y])$ (6)

Decryption: $D(PUkey[m', y])$ (7)

Verification: $y' = H(m', Enode), y == y'$ (8)

Algorithm 1 is used to generate the secret code for each communication. The secret code is unique per device and created using enode of running blockchain node. Each running blockchain nodes have their unique enode id. The secret code is formed by appending enode id along with device's RPC/HTTP address and RPC/HTTP port number. The proposed algorithm prevents any unauthorized data access as well as unauthorized data alternation. The Controller server provides the fine access control mechanism to prevent any kind of the malicious communication from any unauthorized devices. The secret code used as message authentication code (MAC) to preserve the authentication as well as for the data integrity. Here, controller (server) uses advanced encryption standard (AES-256).

Algorithm 1. Secret code generation

```
Sender (IoT Node)
        n ← number of IoT devices
        message ← sensor data
        s ← enode id of Blockchain node      // s is secret code
        for i = 1 to n do
                IP[i] ← IP:Port              // Combining IP address with port
        end for
        Sdata[i] → h(message[i] + s[i])      // Appending message with secret code to create
         hash
for all i do
        send IP[i] ← Sdata[i]         // Send to specific device
end for
Receiver (IoT Controller Node)
        Rdata ← h'(message' + s') // Regenerate hash from received message
        If (Rdata == Sdata) Then // Verify received hash, h and calculate hash, h'
                Set DATA = Rdata // Accept data
        Else
                Set DATA = null // Reject data
        end if
```

4. RESULT AND DISCUSSION

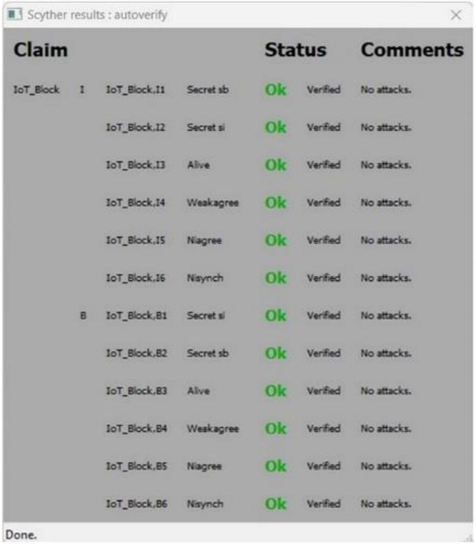
To set up IoT-Blockchain ecosystem, we have used one raspberry pi as IoT device which is light running Blockchain node and one Jetson Nano device having sufficient amount of computing power as IoT controller node to process information. The Jetson Nano node is act as full Blockchain node that store data directly to Blockchain network through smartcontract. There are other three computer systems that act as full Blockchain node. The configuration details are given in Table 2. All the devices are connected through WIFI as well as Ethernet on same network. All the nodes are having proper time synchronization as per the Blockchain network to synchronize the transactions [27]. We have used Scyther tool to verify our algorithm against security flaws. Scyther is a protocol verification tool used to analyze security protocols. It is an automated tool that helps in identifying flaws and vulnerabilities in security protocols before they are deployed in a real-world scenario. The tool supports a wide range of security properties, including confidentiality, integrity, authentication, and non-repudiation. We used Scyther to analyze security including key exchange protocols, authentication protocols, and secure communication protocols. The tool runs the interactions to check the possible vulnerabilities against claims presented in Table 3. The claims are about to evaluate aliveness of source and destination node, authentication in term of weakagree, Niagree and Nisynch. Our main strength of algorithm is the secret code that must be remained secure during the communication. Figure 4 shows the claim that we want to achieve using our proposed algorithm. The entire algorithm has been developed using scythe protocol description language (SPDL) and tested against all possible vulurabalities using autoverfy functionality of tool. The result analysis clearly shows that there is no any attack possible with our proposed algorithm.

Table 2. IoT-blockchain node characteristics

Node	Blockchain node	Blockchain node type	Node role	Unique characteristics
Computer	Yes	Full	Miner/Validator	Enode:RPC/HTTP_Address:RPC/HTTP_Port
Computer	Yes	Full	Miner/Validator	Enode:RPC/HTTP Address : RPC/HTTP Port
Computer	Yes	Full	Miner/Validator	Enode:RPC/HTTP Address : RPC/HTTP Port
Raspberry Pi	Yes	Light	Participant	Enode:RPC/HTTP Address : RPC/HTTP Port
Jetson Nano	Yes	Full	Participant	Enode:RPC/HTTP Address : RPC/HTTP Port

Table 3. Validation result

Claim	Status	Attack	description
claim_i1 (I, Alive) claim_b1 (B, Alive)	Ok	No attack	It ensures authentication to execute some event from intended party, I
claim_i2 (I, Weakagree) claim_b2 (B, Weakagree)	Ok	No attack	It ensures that both the party are actual communicating to each other.
claim_i3 (I, Niagree) claim_b3 (B, Niagree)	Ok	No attack	It ensures that all the party in the communication reach to the same decision.
claim_i4 (I, Nisynch) claim_b (B, Nisynch)	Ok	No attack	All the messages are sent from sender and recived by the party, B.
claim_i5 (I, Secret, sk (I, B)) claim_b5 (B, Secret, k (B, I))	Ok	No attack	It is shared secret between two communicating party, I and B



Scyther results : autoverify

Claim				Status		Comments
IoT_Block	I	IoT_Block,I1	Secret sb	Ok	Verified	No attacks.
		IoT_Block,I2	Secret si	Ok	Verified	No attacks.
		IoT_Block,I3	Alive	Ok	Verified	No attacks.
		IoT_Block,I4	Weakagree	Ok	Verified	No attacks.
		IoT_Block,I5	Niagree	Ok	Verified	No attacks.
		IoT_Block,I6	Nisynch	Ok	Verified	No attacks.
	B	IoT_Block,B1	Secret si	Ok	Verified	No attacks.
		IoT_Block,B2	Secret sb	Ok	Verified	No attacks.
		IoT_Block,B3	Alive	Ok	Verified	No attacks.
		IoT_Block,B4	Weakagree	Ok	Verified	No attacks.
		IoT_Block,B5	Niagree	Ok	Verified	No attacks.
		IoT_Block,B6	Nisynch	Ok	Verified	No attacks.

Done.

Figure 4. Scyther tool for result analysis of vulnerability testing

5. CONCLUSION

The integration of IoT and Blockchain technologies can significantly improve the functionality and security of various smart applications. By leveraging the distributed and immutable nature of Blockchain, IoT nodes transmit data securely without the need for centralized intermediaries. This can help mitigate the risks of data tampering, hacking, and privacy breaches, while also enabling greater transparency and accountability in the smart application ecosystem. In this research, we found data security critical issue from research findings and proposed security algorithm that make entire communication secure without tempering information from IoT device to controller device such as gateway and Blockchain network. The algorithm generates the secure secret code that append with original message generated from IoT devices. The hash of secret code and message is protected using public key cryptosystem elliptical curve cryptography (ECC) and entire information is protected using single secret key using advanced encryption standard (AES). The keys are pre generated and distributed to the target devices. The characteristics of the nodes which are used to identified the legitimate node. Finally, we verified our algorithm using scyther security verifier tool with possible vulnerabilities in term of attacks. We found our algorithm secure for IoT and Blockchain end to end data communication between IoT node to Blockchain network.

REFERENCES

[1] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W. C. Hong, “Internet of things: Evolution, concerns and security challenges,” *Sensors*, vol. 21, no. 5, pp. 1–35, Mar. 2021, doi: 10.3390/s21051809.

[2] S. Khan, R. Singh, S. Khan, and A. H. Ngah, “Unearthing the barriers of Internet of Things adoption in food supply chain: A developing country perspective,” *Green Technologies and Sustainability*, vol. 1, no. 2, p. 100023, May 2023, doi: 10.1016/j.grets.2023.100023.

[3] B. H. Patel and P. Shah, “RPL routing protocol performance under sinkhole and selective forwarding attack: Experimental and simulated evaluation,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 4, pp. 1849–1856, Aug. 2020, doi: 10.12928/TELKOMNIKA.V18I4.15768.

[4] N. Jayashri, V. Rampur, D. Gangodkar, M. Abirami, C. Balarengadurai, and N. A. Kumar, “Improved block chain system for high secured IoT integrated supply chain,” *Measurement: Sensors*, vol. 25, p. 100633, Feb. 2023, doi: 10.1016/j.measen.2022.100633.

[5] S. Anand and A. Sharma, “Comprehensive analysis of services towards enhancing security in IoT-based agriculture,” *Measurement: Sensors*, vol. 24, p. 100599, Dec. 2022, doi: 10.1016/j.measen.2022.100599.

[6] Q. I. Sarhan, “Internet of things: a survey of challenges and issues,” *International Journal of Internet of Things and Cyber-Assurance*, vol. 1, no. 1, p. 40, 2018, doi: 10.1504/ijitca.2018.10011246.

[7] I. Singh and B. Singh, “Access management of IoT devices using access control mechanism and decentralized authentication: A review,” *Measurement: Sensors*, vol. 25, p. 100591, Feb. 2023, doi: 10.1016/j.measen.2022.100591.

[8] M. Touloupou, M. Themistocleous, E. Iosif, and K. Christodoulou, “A systematic literature review toward a blockchain benchmarking framework,” *IEEE Access*, vol. 10, pp. 70630–70644, 2022, doi: 10.1109/ACCESS.2022.3188123.

[9] M. S. Mahmood and N. B. Al Dabagh, “Blockchain technology and internet of things: review, challenge and security concern,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 1, pp. 718–735, Feb. 2023, doi: 10.11591/ijece.v13i1.pp718-735.

[10] Y. Lu, “Implementing blockchain in information systems: a review,” *Enterprise Information Systems*, vol. 16, no. 12, Dec. 2022, doi: 10.1080/17517575.2021.2008513.

[11] J. Liu, H. Zhang, and L. Zhen, “Blockchain technology in maritime supply chains: applications, architecture and challenges,” *International Journal of Production Research*, vol. 61, no. 11, pp. 3547–3563, Jun. 2023, doi: 10.1080/00207543.2021.1930239.

[12] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang, “Blockchain-enabled smart contracts: architecture, applications, and future trends,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[13] S. K. Ezzat, Y. N. M. Saleh, and A. A. Abdel-Hamid, “Blockchain Oracles: State-of-the-art and research directions,” *IEEE Access*, vol. 10, pp. 67551–67572, 2022, doi: 10.1109/ACCESS.2022.3184726.

[14] H. Kim and D. Kim, “A taxonomic hierarchy of blockchain consensus algorithms: an evolutionary phylogeny approach,” *Sensors*, vol. 23, no. 5, p. 2739, Mar. 2023, doi: 10.3390/s23052739.

[15] J. Sengupta, S. Ruj, and S. D. Bit, “A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT,” *Journal of Network and Computer Applications*, vol. 149, p. 102481, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.

[16] F. J. Ferrández-Pastor, J. Mora-Pascual, and D. Díaz-Lajara, “Agricultural traceability model based on IoT and Blockchain: Application in industrial hemp production,” *Journal of Industrial Information Integration*, vol. 29, p. 100381, Sep. 2022, doi: 10.1016/j.jii.2022.100381.

[17] H. H. Khan, M. N. Malik, Z. Konečná, A. G. Chofreh, F. A. Goni, and J. J. Klemeš, “Blockchain technology for agricultural supply chains during the COVID-19 pandemic: Benefits and cleaner solutions,” *Journal of Cleaner Production*, vol. 347, p. 131268, May 2022, doi: 10.1016/j.jclepro.2022.131268.

[18] P. Dutta, T. M. Choi, S. Somani, and R. Butala, “Blockchain technology in supply chain operations: Applications, challenges and research opportunities,” *Transportation Research Part E: Logistics and Transportation Review*, vol. 142, p. 102067, Oct. 2020, doi: 10.1016/j.tre.2020.102067.

[19] U. Sakthi and J. DafniRose, “Blockchain-enabled smart agricultural knowledge discovery system using edge computing,” *Procedia Computer Science*, vol. 202, pp. 73–82, 2022, doi: 10.1016/j.procs.2022.04.011.

[20] F. H. Al-Naji and R. Zagrouba, “CAB-IoT: Continuous authentication architecture based on Blockchain for internet of things,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 2497–2514, Jun. 2022, doi: 10.1016/j.jksuci.2020.11.023.

[21] M. T. Al Ahmed, F. Hashim, S. J. Hashim, and A. Abdullah, “Hierarchical blockchain structure for node authentication in IoT networks,” *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 345–361, Jul. 2022, doi: 10.1016/j.eij.2022.02.005.

[22] M. Al-Shabi and A. Al-Qarafi, “Improving blockchain security for the internet of things: challenges and solutions,” *International Journal of Electrical and Computer Engineering*, vol. 12, no. 5, pp. 5619–5629, Oct. 2022, doi: 10.11591/ijece.v12i5.pp5619-5629.

[23] S. Khanji, O. Alfandi, L. Ahmad, L. Kakkengal, and M. Al-kfairy, “A systematic analysis on the readiness of Blockchain integration in IoT forensics,” *Forensic Science International: Digital Investigation*, vol. 42–43, p. 301472, Oct. 2022, doi: 10.1016/j.fsidi.2022.301472.

[24] G. Ramkumar, K. Kasat, P. R. A. Khader, P. K. N. Muhammed, T. Raghu, and S. Chhabra, “Quality enhanced framework through integration of blockchain with supply chain management,” *Measurement: Sensors*, vol. 24, p. 100462, Dec. 2022, doi: 10.1016/j.measen.2022.100462.

[25] A. Pakseresht, A. Yavari, S. A. Kaliji, and K. Hakelius, “The intersection of blockchain technology and circular economy in the agri-food sector1,” *Sustainable Production and Consumption*, vol. 35, pp. 260–274, Jan. 2023, doi: 10.1016/j.spc.2022.11.002.

[26] M. Parmar and P. Shah, “Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application,” *International Journal of Electrical and Computer Engineering (IJEECE)*, vol. 13, no. 4, pp. 4422–4431, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4422-4431.

[27] 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.

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 has 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 email: 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 master’s degree in computer engineering in 2004, Gujarat, India. He is a Professor at 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 email: parthshah.ce@charusat.ac.in.