Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 7, pp. 2087–2099
DOI : 10.47974/JDMSC-2082

A novel approach for integrating cryptography and blockchain into IoT system

Basetty Mallikarjuna [§]
Department of Information Technology
Institute of Aeronautical Engineering
Dundigal, Hyderabad
Telangana 500043
India

Gagandeep Berar [†]
Department of Computer Science and Engineering
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab 140401
India

Ajit Noonia *
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Lekha Rani [‡]
Department of Computer Science and Engineering
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab 140401
India

[§] *E-mail:* b.mallikarjuna@iare.ac.in
[†] *E-mail:* gagandeep2913@gmail.com
* *E-mail:* ajit009noonia@gmail.com (Corresponding Author)
[‡] *E-mail:* lbhambhu@gmail.com

Chittemsetty Pushpalatha [@]
Department of Master of Business Administration
Institute of Aeronautical Engineering
Dundigal, Hyderabad
Telangana 500043
India

Shiju Sebastian [#]
School of Business and Management
CHRIST University
Delhi NCR Campus
Uttar Pradesh 201003
India

Abstract

The quick advancement of Internet of Things (IoT) emphasizes the significance of cryptography and blockchain ensuring the security of sensitive data and connected devices. Blockchain technology and encryption play key roles in ensuring the security of the expansive IoT network. Blockchain offers decentralized trust, immutability, and transparency to IoT networks and transactions, while encryption serves to protect IoT data from unauthorized access. It is a novel approach for integrating cryptography and blockchain into IoT System, cryptography and blockchain stand out as robust technologies that enhance the security of IoT systems. The implementation of an integrated architecture, along with a strategic integration approach, further strengthens the security measures. This methodology proves valuable for managing and validating digital transactions on decentralized, immutable networks. This work also explores the potential significance of integrating cryptography and blockchain into IoT System, this functions and applications in enhancing IoT security. This methodology introduces encryption techniques tailored for resource-constrained IoT devices, which are essential for ensuring end-to-end security.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Cryptography, Block chain, Integrating approach, Security, IoT, End-to-end security, Privacy.*

1. Introduction

In current digital scenario, IoT has completely revolutionized how devices communicate and interact with each other. It increasing number of connected devices has also given rise to concerns regarding data security

[@] *E-mail:* **ch.pushaplatha@iare.ac.in**
[#] *E-mail:* **shijusebastian@christuniversity.in**

and privacy [1]. To tackle these challenges, the integration of a novel approach for cryptography and blockchain into IoT system, it has emerged as an effective solution. This article examines the synergies between blockchain and cryptography within the realm of IoT, exploring their individual functionalities, advantages, and practical applications [2]. By comprehending the collaborative workings of these technologies, a novel approach for integrating cryptography and blockchain into IoT system of potential hold in enhancing security and trust within IoT ecosystems and provides the end-to-end security. Blockchain technology and cryptography play a vital role in addressing the IoT ecosystem, the security concerns associated with the IoT is a challenging task [3]. By providing decentralized trust and ensuring data integrity that cannot be tampered with, blockchain technology offers a robust solution. Additionally, cryptography offers the necessary tools and protocols to make end-to-end connection within the IoT [4]. The advanced technology of cryptography is a blockchain that enhance the safety and security of IoT installations, effectively protecting both the connected devices and the valuable data they generate in IoT system. The subsequent aims are described below [5].

- Cryptography's robust encryption and authentication mechanisms make it suitable for ensuring access control and securing data communication in the realm of IoT [6].
- To ensure data integrity, privacy and end-to-end security and trust in IoT applications, blockchain offers a decentralized and secure platform. To ensure optimal end-to-end security for their IoT deployments, organizations must conduct assessment of what they require and carefully consider the advantages and disadvantages of all available technologies before making a selection [7].
- The collaboration between blockchain technology and cryptography has the potential developments to enhance the security in IoT systems [8].
- By combining blockchain technology with cryptography, IoT security can be strengthened through secure communication channels, device authentication, and data encryption [9].
- Transaction logs and sensor data are essential types of data integrating cryptography and blockchain into IoT system ensuring their integrity is verified [10].

The danced technology of cryptographic processes can potentially lead to a blockchain, it performs the issues in IoT devices that have incomplete and less resources due to their computational power. Additionally, in large-scale deployments of IoT, managing and distributing keys such as public key/private key can become complex [11]. While blockchain offers decentralization and immutability, the processing of a high volume of IoT transactions can result in latency and scalability challenges and end-to-end security [12]. This article examines the feasibility and trade-offs of incorporating cryptography or blockchain into IoT security architectures, while considering aspects such as end-to-end security, performance, and regularity [13].

The second section of this article presents literature survey and applications, while the third section delves into the proposed methodology and an integrated approach. Moving on to the fourth section, it covers the implementation work, and finally, the fifth section outlines the integrating cryptography and blockchain into IoT system for the conclusion and future work followed by references.

2. Literature Survey

The IoT is developed up of devices that are interconnected, allowing them to freely communicate and exchange data effortlessly [14]. The rapid expansion of IoT has brought about notable end-to-end security and privacy issues, underscoring the importance of implementing strong end-to-end security measures [15]. The advanced cryptography technology provides blockchain technology present viable solutions to bolster the end-to-end security, integrity and reliability of IoT systems [16]. This work developed a novel methodology for incorporating cryptographic methods and blockchain technology into IoT networks [17]. IoT systems encounter numerous security obstacles, which encompass. Data Integrity, guaranteeing that data remains unaltered during transmission [18]. Authentication and Authorization, it validating the identity of devices and managing their access. End-to-end security and Privacy, safeguarding sensitive data against unauthorized entry. Scalability, effectively managing a substantial number of devices while ensuring security measures are in place [19].

The advanced technology of cryptography leads to blockchain into IoT system, it plays a vital role in ensuring the security of IoT by providing various essential tools [20]. The advanced technology of cryptographic methods that are particularly relevant to IoT encompass. Symmetric

encryption performs a single key/shared key for both encryption and decryption processes, It is a crucial part of integrating cryptography and blockchain into IoT System [1]. This approach proves to be efficient and well-suited for IoT devices with limited resources. Prominent algorithms used in symmetric encryption include AES (Advanced Encryption Standard) [2]. Asymmetric encryption performs a set of public and private keys, offering secure key exchange mechanisms despite its higher computational intensity [3]. RSA algorithm and ECC (Elliptic Curve Cryptography) algorithm are extensively to work hidden and utilized in blockchain technology in this regard [4]. Data is transformed into a specific string of characters with a fixed length through hash functions, creating a distinct representation of the initial data [5]. The SHA-256 (Secure Hash Algorithm 256-bit) is frequently performed in blockchain technology and to guarantee the integrity of data and end-end to security [6]. Digital signatures provide authentication and non-repudiation in cryptography that works implicitly in blockchain technology [7]. They use asymmetric encryption to verify the authenticity and integrity of a message. ECDSA (Elliptic Curve Digital Signature Algorithm) is often performed in IoT [8].

Blockchain is a distributed ledger and legitimate technology that provides transparency, immutability, and end-to-end security, which makes it well-suited for IoT applications. Blockchain technology eliminates the necessity of a central authority by dispersing data among numerous nodes to well performed in IoT system [9]. Consequently, this diminishes the likelihood of a solitary point of failure [10]. Once information is recorded on a blockchain, it becomes immutable and cannot be modified or erased, thereby guaranteeing the integrity and traceability of the data [11]. Smart contracts are contracts that execute themselves automatically, with the agreement's terms directly encoded into the code to perform in IoT. They facilitate automated and end-to-end secure interactions between IoT devices [12]. Consensus algorithms guarantee unanimous agreement among all nodes regarding the integrating cryptography and blockchain into IoT system [13]. While various consensus also apply such as Proof of Work (PoW) and Proof of Stake (PoS) are widely used in integrating cryptography and blockchain into IoT system, alternatives Practical Byzantine Fault Tolerance (PBFT) could be better suited for IoT applications due to their reduced energy consumption [14].

In order to incorporate cryptography and blockchain into the IoT, it is essential to perform Public Key Infrastructure (PKI) this is initial stage of blockchain [15]. By utilizing asymmetric cryptography, a secure communication channel can be established between IoT devices and the

network, it performs the layer of blockchain technology [16]. Additionally, device identity verification can be achieved by implementing digital certificates, thereby ensuring the authenticity of the devices [17]. Utilize symmetric encryption for effective and secure communication between devices, implementing end-to-end encryption [18]. Implement blockchain technology for decentralized key management to enhance security and prevent keys from being vulnerable to a single point of attack [19]. Data hashing, it utilize hash functions to authenticate the integrity of data exchanged between devices. Blockchain storage performs the essential data hashes on the blockchain to establish an unalterable log of data integrity [20]. Utilize smart contracts to automate interactions and processes among IoT devices, guaranteeing that actions are carried out solely upon meeting specific conditions [1]. Leverage off-chain storage and computing solutions to manage extensive of data and alleviate the risk on the blockchain utilizing the IoT system [2]. Utilize Layer 2 protocols such as state channels or sidechains to improve scalability and end-to-end security [3].

The convergence of cryptography and blockchain technology in IoT devices has improved the significant growth over time [4]. The integration has advanced from simple implementations to complex, scalable solutions that meet the intricate of cryptography, blockchain and IoT System for security demands of modern IoT ecosystems [5]. In the current digital scenario, it can anticipate further innovations that will enhance the end-to-end security, integrity, privacy, and efficiency of IoT systems [6]. The following figure 1 provides a year-by-year overview of highlighting key developments, the advancement of cryptography and blockchain

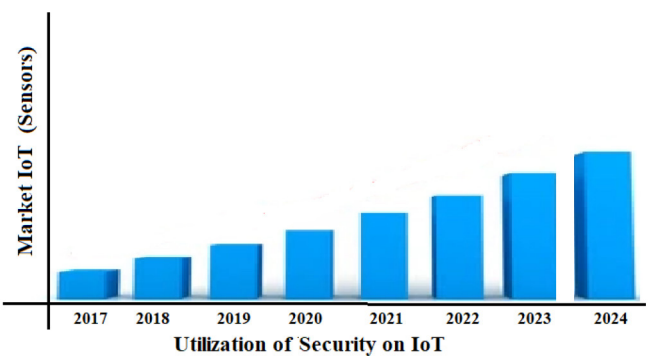

Figure 1

Security on IoT in the market year wise

technology in IoT system and market trends, and technological advancements [7].

The years between 2016 and 2017, there was a rise in cryptography and interest and initial funding of blockchain for proof-of-concept initiatives [8]. The years from 2018 to 2019, there was a huge implementation of cryptography and blockchain technology in supply chain managment, logistics, and industrial IoT, with major investments from technology giants [9]. Throughout the years 2020 and 2021, blockchain technology became widely accepted across various industries and enhancements of IoT systems, focusing on high-quality solutions and structures for businesses [10]. In the years 2022 to 2023, there was an expansion into new applications such as smart cities, healthcare, and autonomous vehicles, due to improvements in scalability and compatibility of blockchain technology [11]. By 2024, blockchain technology had been widely adopted in all sectors, with ongoing advancements in cryptographic methods and integration techniques of IoT systems [12].

3. Proposed Methodology

Integrating the IoT architecture with cryptography and blockchain can greatly improve the end-to-end security, integrity, transparency, and reliability of IoT systems. Integrating cryptography and blockchain with IoT architecture enhances the integrity, end-to-end security, transparency, and immutability of the data collected from IoT devices. The following figure 2 illustrates a simple implementation that has the potential to be

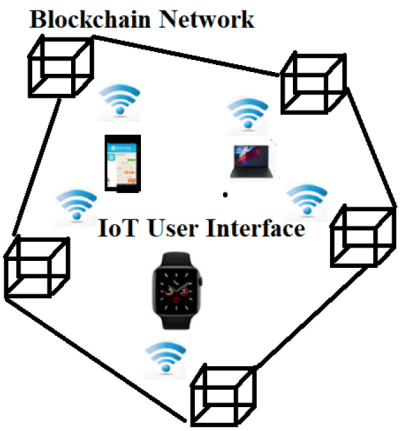

Figure 2

Blockchain with IoT Architecture

expanded to encompass more sophisticated features like advanced data analytics, automated responses via smart contracts, and seamless integration with cloud services to create a comprehensive IoT ecosystem. The step by step detailed explanation given below.

Step 1: Connectivity of IoT Devices, Sensors/Actuators:

Gather through the information from IoT sensors that surrounding environment or carry out specific tasks.

Step 1a: Communication Modules: Facilitate connectivity to IoT devices (such as Wi-Fi, Zigbee, and LoRa) and integrate to run on smart contract.

Step 2: Gateway:

Step 2a: Data Aggregation in Gateway: Gather data from IoT devices and perform to run on smart contract.

Step 2b: Initial Processing through Gateway: Filter and preprocess the data before transmitting it to the integrating cryptography and blockchain into IoT network.

Step 2c: Blockchain Client act in Gateway: Interface for integrating cryptography and blockchain into IoT System.

Step 3: Nodes: Distributed nodes that validate transactions and maintain the blockchain ledger.

Step 3a: Smart Contracts act as various Nodes: Autonomous programs can execute cryptography and blockchain into IoT network.

Step 3b: Decentralized Storage in Nodes: Distributed storage for IoT data.

Step 4: Cloud Services:

Step 4a: Data Analytics in Cloud Service: Advanced cryptography such as blockchain and machine learning services to extract visions from IoT.

Step 4b: Application Services of Cloud: User interfaces, dashboards, and other services tailored to specific applications.

This process of methodology works for three steps, connecting the IoT devices through the gateway to the blockchain nodes and perform through the cloud services. Data is collected by IoT devices and transmitted to the gateway for further processing. The gateway then preprocesses the data and communicates with the blockchain nodes. Transactions are

generated by the gateway and transmitted to the advanced cryptography of blockchain network. Smart contracts are executed in response to incoming transactions in the block chain. Authenticated data is stored on the blockchain, and cloud services can be utilized for additional data analysis.

The smart contract outlines a basic framework for storing IoT data on the blockchain and includes methods for adding and fetching data as per aforementioned steps. Interacting with the blockchain involves a Python script that utilizes web3 to establish a connection through a gateway as per step 2, create and authorize a transaction for adding IoT data, and subsequently submit this transaction to the blockchain as per step 3. Upon completion of the transaction, the script pauses for the mining process to finish before retrieving the data stored to confirm its successful addition to the blockchain to provide end-to-end security, privacy and intigrity.

4. Implementation

In order to showcase the fusion of cryptography and blockchain within an IoT framework, we have the ability to craft Python code excerpts that exhibit essential features like device verification through cryptography, encrypted communication, and the incorporation of blockchain via smart contracts. The step by step procedure as follows.

Step 1: Digital Signatures for Device Authentication

Digital signatures are crucial for verifying the authenticity and security and integrity of devices that are part of an IoT. It performs the security of communication and validating the legitimacy of devices within an IoT ecosystem. It can run on following sub steps.

- **Key Generation:** The device generates a pair of ECDSA keys, with the private key being kept confidential and the public key being shared with the server.
- **Message Signing:** Using ECDSA, the device signs a message with its private key. Subsequently, the signature, along with the message, is transmitted to the server.
- **Serialization:** Both private key and public key and the signature undergo serialization. The public key/private key is serialized to PEM format (it is in the form of certificate), which facilitates easy transmission and storage. On the other hand, the signature is serialized to bytes.

Figure 3

Blockchain within the realm of IoT

- **Verification:** The server loads the public key/private key, receives the message and the signature, decodes the signature, and proceeds to verify it using the public key/private key. If the authentication and verification process is successful, it confirms the authenticity of the message, indicating that it was indeed sent by the legitimate IoT device.

Step 2: Communication secured through the use of symmetric encryption.

It is in the form of cryptography that utilize the cryptography library to perform encryption and decryption of a message by employing AES encryption.

Step 3: Basic Blockchain Implementation for Ensuring IoT Data Integrity.

It is in the form of blockchain that utilize the blockchain library to construct a basic blockchain for the purpose of storing IoT data as shown in Figure 3.

Figure 3 laptop shows the block 0 (geniuses block, it is a first block because previous hash value zero) and block 1 timestamp data, hash key value, previous hash value, that demonstrate the integration of advanced cryptographic techniques and blockchain for enhancing IoT security. By using these methods, IoT systems can ensure secure communication, data integrity, and trustless automation.

5. Conclusion and Future Enhancements of this work

The incorporation of integrity cryptography and blockchain technology into the IoT offers a strong framework to tackle end-to-end

security, integrity and privacy concerns. Through the utilization of these advancements achieved through the end-to-end security, IoT systems can attain improved data integrity, reliable authentication and privacy, and automated interactions without the need for trust. This integration approach establishes to run the smart contract for a secure and expandable IoT ecosystem.

For future enhancements and various practical implementations showcase the merging of cryptography and blockchain into the IoT system. This is the most wanted application in Supply Chain Management (SCM), blockchain guarantees the traceability and legitimacy of products along the supply chain, with cryptography and blockchain are most useful in data transmission for IoT. Smart homes benefit from secure communication and authentication protocols that shield smart devices from unauthorized entry, they need end-to-end security, privacy and integrity. In the healthcare sector, blockchain is most wanted for patient information and verifies its accuracy, while advanced cryptographic methods useful for uphold privacy, end-to-end security and privacy.

References

[1] S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. Annane, "Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing," *The Journal of Supercomputing*, vol. 80, no. 3, pp. 3738-3816 (2024).

[2] B. Mallikarjuna, "Feedback-based fuzzy resource management in IoT-based-cloud," *International Journal of Fog Computing* (IJFC), vol. 3, no. 1, pp. 1-21 (2020).

[3] S. Tanwar, N. Gupta, C. Iwendi, K. Kumar, and M. Alenezi, "Next generation IoT and blockchain integration," *Journal of Sensors* (2022).

[4] D. K. Sharma, A. K. Kaushik, A. Goel, and S. Bhargava, "Internet of things and blockchain: integration, need, challenges, applications, and future scope," in Handbook of Research on Blockchain Technology, pp. 271-294. Academic Press (2020).

[5] B. Mallikarjuna, "Feedback-based resource utilization for smart home automation in fog assistance IoT-based cloud," in Research Anthology on Cross-Disciplinary Designs and Applications of Automation, pp. 803-824. IGI Global (2022).

[6] W. Yan, N. Zhang, L. L. Njilla, and X. Zhang, "PCBChain: Lightweight reconfigurable blockchain primitives for secure IoT applications," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 10, pp. 2196-2209 (2020).

[7] P. Zhang, Y. Wang, G. S. Aujla, A. Jindal, and Y. D. Al-Otaibi, "A blockchain-based authentication scheme and secure architecture for IoT-enabled maritime transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2322-2331 (2022).

[8] Z. Iftikhar, Y. Javed, S. Y. A. Zaidi, M. A. Shah, Z. I. Khan, S. Mussadiq, and K. Abbasi, "Privacy preservation in resource-constrained IoT devices using blockchain—A survey," Electronics, vol. 10, no. 14, p. 1732 (2021).

[9] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 491-498 (2019).

[10] R. Akkaoui, "Blockchain for the management of internet of things devices in the medical industry," *IEEE Transactions on Engineering Management*, vol. 70, no. 8, pp. 2707-2718 (2021).

[11] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, "An enhanced quantum key distribution protocol for security authentication," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 4, pp. 499-507 (2019).

[12] N. Janu, A. Kumar, L. Raja, V. Bhatnagar, A. Kumar, S. Kumar, and R. C. Poonia, "Development of an efficient real-time H.264/AVC advanced video compression encryption scheme," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 8, pp. 2245-2255 (2021).

[13] M. Kassab, J. DeFranco, T. Malas, P. Laplante, G. Destefanis, and V. V. Graciano Neto, "Exploring research in blockchain for healthcare and a roadmap for the future," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1835-1852 (2019).

[14] A. Altameem, B. Mallikarjuna, A. K. Jilani Saudagar, M. Sharma, and R. C. Poonia, "Improvement of automatic glioma brain tumor detection using deep convolutional neural networks," *Journal of Computational Biology*, vol. 29, no. 6, pp. 530-544 (2022).

[15] S. Pal, T. Rabehaja, M. Hitchens, V. Varadharajan, and A. Hill, "On the design of a flexible delegation model for the Internet of Things using blockchain," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3521-3530 (2019).

[16] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 491-498 (2019).

[17] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications," *IEEE Transactions on Engineering Management,* vol. 67, no. 4, pp. 1256-1270 (2020).

[18] B. Mallikarjuna, S. Addanke, and D. J. Anusha, "An improved deep learning algorithm for diabetes prediction," in Handbook of Research on Advances in Data Analytics and Complex Communication Networks, pp. 103-119. IGI Global (2022).

[19] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, "An enhanced quantum key distribution protocol for security authentication," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 4, pp. 499-507 (2019).

[20] B. Mallikarjuna, "An effective management of scheduling-tasks by using MPP and MAP in smart grid," *International Journal of Power and Energy Conversion*, vol. 13, no. 1, pp. 99-116 (2022).

Received March, 2024