Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 7, pp. 2015–2025
DOI : 10.47974/JDMSC-2076

Comparing the roles of cryptography and blockchain technology in relation to Internet of Things

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

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

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

Kailash Nath Tripathi [@]
Department of Computer Engineering
ISBM College of Engineering
Pune 411042
Maharashtra
India

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

© Taru Publications

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

Abstract

Cryptography and blockchain technology are super important for keeping all our smart devices safe in the Internet of Things (IoT) which can be considered as social security. As more and more of our gadgets connect to the internet, we really need to make sure they're secure. This article talks about how we can use blockchain technology with IoT devices. Introduction and literature survey provides the challenges of having cryptography and blockchain technology in relation to Internet of Things, the proposed methodology provides the limited internet speed, and how blockchain affects how fast our devices can work and compare the cryptography attributes and blockchain technologies with the IoT world. To maintain the data safe and securely and provide the integrity and provide the high throughput, the Weight Allocation Authority (WAA) gives priority to users based on their characteristics. The Secure Hash Algorithm-512 helps make bigger data smaller. This work deals with the Hybrid Weighted Algorithm (HWA) and how IoT devices can improve the faster data transmission securely. WAA and HWA algorithms canalso create a safe and decentralized system that can quickly stop any bad transactions.

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

Keywords: *Cryptography, Block chain, Security, IoT, Integrity, Privacy.*

1. Introduction

Cryptography helps to works save guard can transmission of data sender to receiver. It converts the encryption to decryption, it also transmits the data securely [1]. The cryptographic key plays a major role, it concealed by an invisible shield and individual processing the sender and receiver. Cryptography and blockchain technology emerge as the trendsetter in the digital realm in relation to Internet of Things to enhance the transparency and security [2]. Blockchain technology works immutable digital ledger and decentralized and visible to all yet impervious to tampering. The Internet of Things empowers everyday objects with communication abilities [3]. The IoT objects like laptop, fans, washing machines with phones to ordering groceries, it creates a sophisticated network where

[#] *E-mail:* **shijusebastian@christuniversity.in**

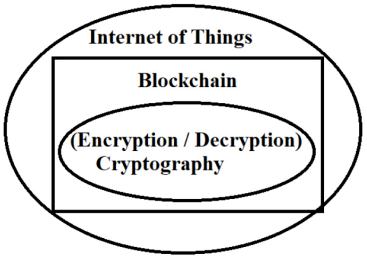


Figure 1

Cryptography Vs Blockchain in the context of IoT

devices interact and exchange information [4]. The IoT and blockchain provides the interconnected environment, security acts as the gatekeeper at the IoT gathering, preventing unauthorized access to smart homes and smart cities [5]. Cryptography acts as the guardian angel of blockchain and IoT, ensuring data remains secure and accessible solely to authorized individuals in cryptography and blockchain technology in relation to Internet of Things. It acts as the digital lock and key, the core layer of cryptography surrounded by the blockchain and it surrounded by the thwarting malicious internet as shown in Figure 1[6].

Blockchain technology is the advanced concepts of cryptography, for secure transmission data in IoT sensors, cryptographic rules act as guardian of IoT devices. IoT data transmission to enforcing cryptographic rules, verifying identities, and internet objects to ensuring that only trusted connections are allowed [7]. In IoT sensors to securely access the VIP data, blockchain with IoT safeguarding it from unauthorized access. In the realm of IoT security, blockchain emerges as a superior in the current scenario [8]. Blockchain technology establishing a decentralized and tamper-proof to provide IoT network, it provides the safety and integrity of IoT data, acting as a digital fortress for smart devicesand smart homes [9]. Smart contracts play the role of digital agreements, ensuring compliance with rules within the IoT ecosystem [10]. It provides the automate processes, foster trust, and maintain smooth operations, to the invisible hand of blockchain governance with cryptography n relation to Internet of Things [11]. Scalability and integrity poses a significant challenge for cryptographic solutions in IoT. As the number of connected devices grows, traditional cryptographic methods struggle to keep pace. Cryptography and blockchain technology in relation to IoTis a challenging issue and keyhole and highly impractical [12]. In cryptography key management in the realm of IoT security presents another hurdle,

cryptography and blockchain having a collection of keys without knowing which one corresponds to each device. Ensuring that in IoT all devices possess the correct keys to apply cryptographic protocols and keeping them security, it notso easy task. Blockchain technology as a digital ledger, recording every transaction and making tampering nearly impossible [13]. Trust issues find resolution in the presence of blockchain [14]. Cryptography and blockchain technology in relation to IoT with supply chain management, blockchain can work wonders in supply chain management. Cryptography and blockchain technology in relation to IoT simplifies the tracking of products from manufacturer to consumer through transparent and immutable record-keeping. No more disappearing shipments with cryptography and blockchain technology in relation to IoT provides thedubious transactions [15].

The security challenges posed by the IoT can be effectively addressed through the use of cryptography and blockchain technology [16]. Cryptography and blockchain technology in relation to IoT integrated with installations, these technologies contribute to a safer and more secure environment [17]. The interplay between cryptography, blockchain technology, and the IoT offers a promising opportunity to enhance security in the current digital scenario [18]. Cryptography and blockchain technology capitalizing on the strengths of these technologies and overcoming their respective obstacles, the integrated technology can establish a more secure and reliable IoT landscape [19]. As advancements in security protocols continue to emerge through innovation of cryptography and blockchain technology in relation to IoT, the fusion of cryptography and blockchain holds immense potential in strengthening IoT ecosystems Weight Allocation Authority (WAA) provides security of various attributes and protecting sensitive data hybridized weighted attribute (HWA) in an increasingly interconnected world [20-22].

This work follows the section 2 gives the short literature review and section 3 discusses proposed methodology of integrated approach and section 4 provides implementation work and section 5 describes conclusion and future work.

2. A Short Literature Review

Cryptography and blockchain technology in relation to IoT ecosystem has brought forth a new era of interconnected digital advancement [1]. Within this rapidly evolving landscape and integrity the fusion of these technologies possesses significant potential to transform data security,

privacy, scalability, integrity and transactions [2]. Cryptography and blockchain technology in relation to IoT with its robust encryption techniques, serves as the bedrock of secure communication and data protection in the current digital scenario. The advanced technology of cryptography is a blockchain technology, the relation in IoT offers a decentralized and tamper-proof platform for the storage and management of data, guaranteeing transparency and integrity in transactions [3]. Cryptography plays a major role secret of data transmission of language of the digital realm, secure data transmission from individually by encoding/ decoding it in a manner that only authorized individuals can comprehend [4, 5].

The history of cryptography and blockchain technology in relation to IoT has evolved significantly, starting from the use of basic substitution ciphers by ancient civilizations to the development of sophisticated encryption algorithms in the present day [6]. Cryptography and blockchain technology in relation to IoT has been evident in various contexts such as warfare, secure data transmission, where it serves as the foundation for secure communication and online transactions [7]. In the realm of technology, blockchain stands as a digital ledger that securely records transactions across a network of computers in a transparent manner [8]. Cryptography and blockchain technology in relation to IoT inclusion of cryptography within blockchain ensures that the data stored in blocks remains unaltered and can be verified, thereby upholding the integrity, scalability, security, and reliability of the information [9]. Cryptography plays a vital role in blockchain technology by facilitating the creation of digital signatures, verifying identities, and safeguarding transactions [10]. Cryptography and blockchain technology in relation to IoT preserving the immutability of the blockchain, cryptography effectively trust worthyof any attempts by malicious individuals to manipulate records or engage in fraudulent activities [11].

3. Proposed Methodology

An IoT application has the power to transform every aspect of a person's everyday life. These areas can be divided into categories such as healthcare, transportation, getting around, making your home super smart, keeping things organized, connecting with friends,. To meet the requirements, special sensors and actuators to collect and share information with other devices. The sensors are tiny and don't need a lot of fancy equipment to work. Sensors, which are small and require minimal

hardware, are an essential part of IoT devices. IoT devices generally have diverse capabilities and hardware.

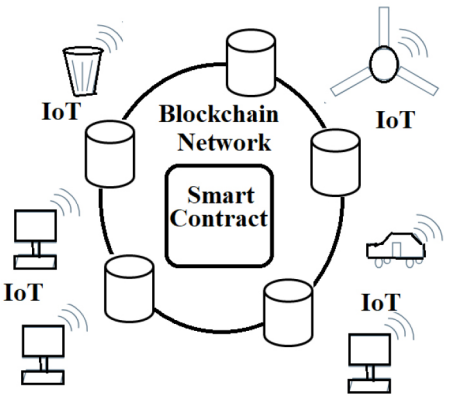


Figure 2

Blockchain with IoT

Figure 2 shows the architecture of Blockchain with IoT. Wireless mesh and ad hoc networks, including Zigbee, support effective communication. These sensors require minimal battery power to function, a crucial requirement. Recently, an innovative communication technology called narrowband internet of things (NB-IoT) has entered the market, it has been implemented to prolong the sensor's lifespan. However, these sensors still have limited processing, storage, and communication capabilities. On the other hand, certain IoT devices like vehicles and mobile phones are both expensive and powerful, equipped with larger batteries and high computing capabilities, as well as ample storage capacity. Subsequently, these devices can run at the highest capacity allowed.

3.1 *Different industries have discovered numerous uses for Blockchain and Internet of Things (IoT).*

The Internet of Things (IoT) network is known for its data-centric nature, with a multitude of sensors or end devices transmitting substantial amounts of data. This heightened data flow exposes vulnerabilities in both the devices and the data itself, making them prime targets for potential attacks within the IoT realm. The information collected by IoT sensors is often sensitive, sometimes even personal. For instance, it could involve a patient's medical records (in medical IoT applications) or data

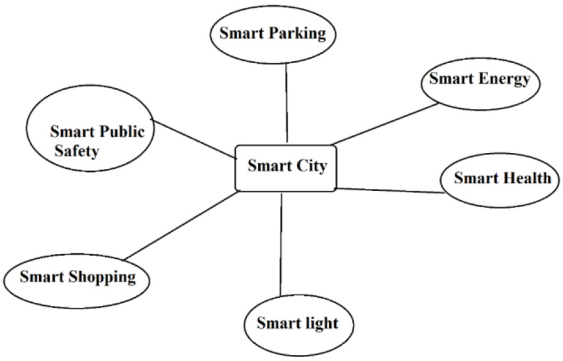


Figure 3

Various application of smart city

related to critical national infrastructure that must be safeguarded (such as smart grid systems or nuclear power plants). Keeping the security and confidentiality of this data is top priority.The crucial maintenance of integrity is facilitated by blockchain technology, reliability, and security of IoT data.At present, numerous applications have been created utilizing IoT technology, including smart city infrastructure as shown in Figure 3, supply chain management, and bitcoin management. It is imperative for these technologies to address security concerns related to both end devices and sensor data.

4. Implementation

The administrator calls the functions for public parameters. The sender calls the security key (SK) parameters and calls the private key (PK), encrypted attributes and Central Authority (CA). Upon verification of the user attributes by the CA, and if deemed valid, the CA uses the PK and SK for new user. In the event that a user is found to have a false identity, not generated the key pair. Advanced standard encryption techniques are utilized for encryption and decryption. The Weight Allocation Authority (WAA) assigns for priority attributes. The Secure Hash Algorithm-512 is to reduce the large data to small data. This technique provides the high levels of security. It is suitable for real-time applications. The encryption in the proposed system ensures precise access control, resistance to collusion, and supports multiple authorities. At a systemic level, the operations of the proposed system are detailed,

including system setup, user registration, user data collection, and new file generation, for new file retrieve, and new file transmission.

4.1 *The functioning of the algorithm plain/cipher text, hybridized weighted attribute (HWA-Algorithm)*

The HWA-Algorithm is an effective solution for achieving these objectives. The attribute-based encryption (ABE) algorithms handles the public key (PK) and secret key (SK), the user performs the multiple authorities. The use sends the data to the associated user and sends the secure and confidential messages. The message transmission tree ensures to update the cipher text to plain text. This system assigns weights to the attributes to ensure the data security and privacy of the user.The advanced security algorithms and encryption/decryption algorithms are used. The Weight Allocation Authority (WAA) performs the user attributes. The Secure Hash Algorithm-512 consumes the large data into the small data.It is suitable for real-time applications. This solution works for access control, resistance to collusion, and convers the cipher txt to plain text and plaint text cipher text

4.2 *Throughput Computation*

The ratio between the file size and WAA/HWA, it referred as throughput. It divide the total plaintext/ciphertext in kilobytes by the total encryption time for the algorithm, as depicted in Figure 4.

$$\text{Throughput} = \frac{FileSize}{WAA/HWA}$$

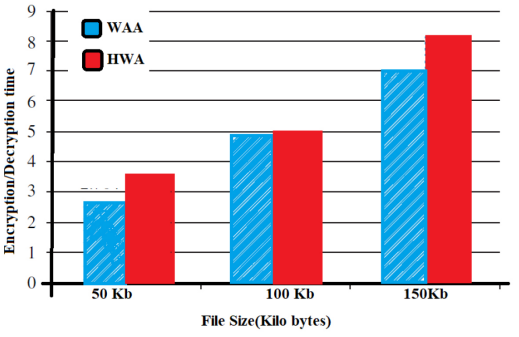


Figure 4

Throughput comparison between WAA and HWA

5. Conclusion and Future Directions

This workexamine the integration of cryptography referred to blockchain towards to relevant of IoT devices. This work also focuses on the challenges posed by the large number of devices, limited communication bandwidth, and the impact of blockchain on computing power. The analysis also includes a comparison of current blockchain technologies with the IoT environment. To enhance data security and privacy, the addition of WAA, HWA for security attributes to the blockchain is investigated, revealing its ability to reduce computational requirements and increase throughput. By implementing this algorithm in the blockchain, a decentralized and secure system can be achieved, enabling prompt action to be taken against any detected illegal transactions.

References

[1] Li, S., Qin, T., & Min, G. Blockchain-based digital forensics investigation framework in the internet of things and social systems. *IEEE Transactions on Computational Social Systems*, 6(6), 1433-1441 (2019).

[2] Dai, Hong-Ning, Zibin Zheng, and Yan Zhang. "Blockchain for Internet of Things: A survey." *IEEE internet of things journal* 6.5 : 8076-8094 (2019).

[3] Viriyasitavat, Wattana, Li Da Xu, Zhuming Bi, and Danupol Hoonsopon. "Blockchain technology for applications in internet of things—mapping from system design perspective." *IEEE Internet of Things Journal* 6, no. 5 : 8155-8168 (2019).

[4] Yousefi, Samuel, and Babak Mohamadpour Tosarkani. "Exploring the role of blockchain technology in improving sustainable supply chain performance: a system-analysis-based approach." *IEEE Transactions on Engineering Management* (2023).

[5] Ma, Mingxin, Guozhen Shi, and Fenghua Li. "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario." *IEEE access* 7 : 34045-34059 (2019).

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

[7] Bera, Basudeb, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, Pascal Lorenz, and MamounAlazab. "Blockchain-envisioned secure data

delivery and collection scheme for 5g-based iot-enabled internet of drones environment." *IEEE Transactions on Vehicular Technology* 69, no. 8 : 9097-9111 (2020).

[8] Viriyasitavat, Wattana, Li Da Xu, Zhuming Bi, and Danupol Hoonsopon. "Blockchain technology for applications in internet of things—mapping from system design perspective." *IEEE Internet of Things Journal* 6, no. 5 : 8155-8168 (2019).

[9] Yan, Wei, Ning Zhang, Laurent L. Njilla, and Xuan Zhang. "PCB Chain: Lightweight reconfigurable blockchain primitives for secure IoT applications." *IEEE Transactions on Very Large Scale Integration* (VLSI) Systems 28, no. 10 : 2196-2209 (2020).

[10] Zhang, Peiying, Yaqi Wang, Gagangeet Singh Aujla, Anish Jindal, and Yasser D. Al-Otaibi. "A blockchain-based authentication scheme and secure architecture for IoT-enabled maritime transportation systems." *IEEE Transactions on Intelligent Transportation Systems* 24, no. 2 : 2322-2331 (2022).

[11] Mallikarjuna, Basetty, Kuppani Sathish, P. Venkata Krishna, and R. Viswanathan. "The effective SVM-based binary prediction of ground water table." *Evolutionary Intelligence* 14, no. 2 : 779-787 (2021).

[12] Altameem, Ayman, Basetty Mallikarjuna, Abdul Khader Jilani Saudagar, Meenakshi Sharma, and Ramesh Chandra Poonia. "Improvement of automatic glioma brain tumor detection using deep convolutional neural networks." *Journal of Computational Biology* 29, no. 6 : 530-544 (2022).

[13] Halgamuge, Malka N., Geetha K. Munasinghe, and Moshe Zukerman. "Time estimation for a new block generation in blockchain-enabled internet of things." *IEEE Transactions on Network and Service Management* (2023).

[14] Mallikarjuna, Basetty, D. Kiranmayee, Vankadara Saritha, and P. Venkata Krishna. "Development of efficient e-health records using IoT and blockchain technology." In ICC 2021-IEEE International Conference on Communications, pp. 1-7. IEEE (2021).

[15] Pal, Shantanu, Tahiry Rabehaja, Michael Hitchens, Vijay Varadharajan, and Ambrose Hill. "On the design of a flexible delegation model for the Internet of Things using blockchain." *IEEE Transactions on Industrial Informatics* 16, no. 5 : 3521-3530 (2019).

[16] Mallikarjuna, Basetty, R. Viswanathan, and Bharat BhushanNaib. "Feedback-based gait identification using deep neural network classification." J Crit Rev 7, no. 4 : 2020 (2019).

[17] Mallikarjuna, Basetty. "The effective tasks management of workflows inspired by NIM-game strategy in smart grid environment." *International Journal of Power and Energy Conversion* 13, no. 1 : 24-47 (2022).

[18] Mallikarjuna, Basetty, Supriya 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] Kumar, Ankit, et al. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 491-498 (2019).

[20] Mallikarjuna, Basetty. "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).

[21] Goyal, Mohit, and Durgesh Srivastava. "A behaviour-based authentication to internet of things using machine learning." *Design and Development of Efficient Energy Systems* : 245-263 (2022).

[22] Kumar, A., Dadheech, P., Singh, V., Raja, L., & Poonia, R. C. An enhanced quantum key distribution protocol for security authentication. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(4), 499-507 (2019).

Received March, 2024