MACHINE INTELLIGENCE RESEARCH
ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

ENHANCE SECURED ACCESS POLICIES TO INTERNET OF THINGS RESOURCES USING THE BLOCKCHAIN ALGORITHM

Yogesh Chandrakant Khairnar
Department of Computer Science and Engineering, Research Scholar, Madhyanchal Professional University, Bhopal, MP (India), kyogesh444@gmail.com

Nagesh Salimath
Professor, Department of Computer Science & Engineering, Madhyanchal Professional University, Bhopal, MP (India), drnageshsalimath84@gmail.com

Abstract
Internet of Things (IoT) is an emerging technology that has attracted considerable attention in recent years due to its wide range of applications. The development of IoT devices has brought new challenges to the field of security and privacy protection. This paper presents a novel approach to enhancing the access control mechanism for Internet of things, leveraging blockchain technology and inner product encryption to establish a robust and secure information service platform. The proposed approach is based on a blockchain-based access control scheme that combines blockchain technology with hashing to provide a greater level of threat mitigation via the suggested approach, all without the need for complex encryption. To validate the proposed solution, a practical test-bed comprising four prototypes of Network Operating Systems (NOSs) has been employed. Performance indices such as computing effort, storage overhead, and latency have undergone evaluation, affirming the viability and effectiveness of the designed solution.
Keywords: - IoT; data access control; broadcast encryption; blockchain; Ethereum platform

Introduction

The dynamic, massive, and lightweight properties of Internet of Things (IoT) device nodes create intricate application environments. Existing access control mechanisms are ill-suited for the evolving security needs of the IoT. While attribute encryption schemes offer fine-grained access control, they may compromise user privacy. This paper introduces a novel IoT access control mechanism that combines blockchain and inner product encryption [1]. The use of blockchain technology addresses the challenges by providing distributed and decentralized access control management, eliminating single points of failure [2]. The tamper-evident nature of blockchain ensures the integrity of ciphertext stored in third-party storage. Smart contracts embedded in the blockchain not only prevent malicious user access but also offer automatic and traceable access control. Furthermore, inner product encryption enables precise access control and complete concealment of access policies[3]. The synergy of blockchain and inner product encryption results in an efficient, secure mechanism that aligns with the access control requirements of the IoT. The challenge of implementing robust access control for IoT devices is unfortunately widespread. Many IoT devices lack the computing resources needed for intensive cryptography, and some are unable to perform any cryptographic functions at all. Additionally, the diverse nature of IoT devices poses difficulties in developing customized authentication protocols. While a scheme may function effectively within a specific protocol, it may fail when applied to others, limiting its compatibility[4]. Moreover, as the IoT architecture transitions from a centralized

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

model to a decentralized one, defining a trust model becomes increasingly complex. In a decentralized environment without a central governing party, addressing access control issues becomes more challenging. The emergence of blockchain technology, initially renowned for its association with Bitcoin, has introduced decentralization to various non-cryptocurrency sectors, including IoT[5,6,7,8,9]. Researchers consider blockchain the 'missing link' capable of establishing a decentralized platform for IoT, where multiple entities collaboratively share data and resources. Furthermore, the advent of smart contracts has enhanced this decentralized environment by enabling adopters to enforce trust in a verifiable manner. Smart contracts also contribute to automating time-consuming IoT workflows, thereby enhancing overall efficiency in the IoT ecosystem. Given these advantages, we contend that blockchain stands out as a suitable platform candidate for constructing an access control system for IoT. An inevitable trend in the Internet of Things (IoT) is the shift from centralized management to a distributed approach. While this transition offers advantages such as reduced overall latency in IoT workflows and real-time processing capabilities, it introduces challenges to access control. In a centralized architecture, IoT data is collected from various devices in the field and stored in a centralized database in the Cloud. Access control is then applied centrally from the Cloud when sharing this data with other parties through an open Application Programming Interface (API). Conversely, in a decentralized environment, resources and data can be shared arbitrarily, necessitating the dispersion of access control procedures across multiple actors, resulting in increased system complexity. Furthermore, in a distributed IoT system, the traditional roles of clients and servers are inverted. With protocols like CoAP or MQTT, IoT services and users must now initiate data requests to IoT devices through gateways or brokers. Consequently, IoT devices assume a passive role, responding to queries from the gateway or broker. This dynamic emphasizes the significance of IoT gateways and underscores the need for a robust access control mechanism for each IoT endpoint in the network [11,12,13,14]. The rest of the article is organised as follows: in Section II, related work; in Section III, methodology of key generation; in Section IV, experimental analysis; and finally, conclusion in Section V.

II. Related work

The integration of blockchain technology into IoT applications has garnered significant attention from researchers. This interest stems from the inherent decentralization associated with blockchain, wherein efficiency, security, and privacy are considered fundamental elements for fostering widespread growth and adoption of IoT scenarios in daily life. As a result, researchers have conducted numerous studies to explore the integration of blockchain and IoT, specifically focusing on smart home applications and, more broadly, smart cities. A recently proposed algorithm based on blockchain technology integration with different approaches is described here. In [1], the authors utilize the Raft consensus algorithm to enhance the throughput of blockchain while addressing the network scalability issue with the Blockchain Distributed Network. The authors utilize the Raft consensus algorithm to enhance the throughput of blockchain while addressing the network scalability issue with the Blockchain Distributed Network. Privacy is one of the most significant problems with IoT networks. They propose utilizing a unique public key encryption generated from a ring signature to implement a

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

blockchain-based anonymous data-sharing method (BA-DS). They propose a blockchain-based anonymous data-sharing method (BA-DS) by utilizing a unique public key encryption generated from a ring signature. In terms of computational complexity, communication overhead, and blockchain use, our suggested BA-DS achieves respectable efficiency. in [3] implemented protocol as a smart contract to facilitate collaboration among various Internet of Things entities, including IoT domain owners, IoT devices, IoT gateways, IoT suppliers, IoT services, IoT consumers, and Internet Service Providers (ISPs). In order to facilitate collaboration among various Internet of Things entities, including IoT domain owners, IoT devices, IoT gateways, IoT suppliers, IoT services, IoT consumers, and Internet Service Providers (ISPs), we have implemented our protocol as a smart contract. in [4] argues that the usage of blockchain in scenarios where multiple stakeholders own applications and IoT platforms can guarantee the synchronisation of the distributed system and its resistance to tampering. When multiple stakeholders own applications and IoT platforms, the use of blockchain will guarantee the distributed system's synchronisation and resistance to tampering. By utilizing a test bed, we verify the methods and suggested architecture. In [5], the proposed DELM method produced amazing outcomes, with an accuracy of 93.91 percent. The findings gained show promise, and we are actively investigating extensions by applying additional datasets and different architectures. [6] integrates these two areas by predicting the security of decentralised blockchains using LSTM networks. In this study, we integrate these two areas by predicting the security of decentralised blockchains using LSTM networks. With a 95.85% accuracy rate, the LTSM technique utilised by the present system to encrypt passwords is effective enough to counteract contemporary threats like man-in-the-middle attacks (MITM) and denial-of-service attacks. In [7], the proposed scheme's primary objectives and unique feature are the implementation of a machine-learning and blockchain-enabled medicine supply chain and recommendation system, which consists of two modules. Our suggested scheme's primary objectives and unique feature are the implementation of a machine-learning and blockchain-enabled medicine supply chain and recommendation system, which consists of two modules. in [8] compares the scalability, distribution, security, privacy, user-centricity, and policy enforcement of the systems. We compare the scalability, distribution, security, privacy, user-centricity, and policy enforcement of the systems. We also offer classifications for access control. We conclude by outlining the difficulties and potential research areas for creating decentralised access control systems for Internet of Things devices. In [9], the authors suggest a unique smart agent design that draws inspiration from the idea of smart contracts. In particular, a fully decentralised, privacy-preserving, and equitable deep-learning blockchain framework is built based on the suggested smart agent. In this framework, every smart agent participates in the FL task, and the agent network is consistent with the blockchain network. In [10], the authors suggested the system's performance with varying user counts. This article is to assist supply chain practitioners in utilising cutting-edge technologies. It will also assist the industry in formulating regulations in accordance with ADL's projections. [11] proposes BacCPSS, a blockchain-based access control system, as a solution to protect privacy in CPSS big data. In order to protect privacy in CPSS big data, this article suggests BacCPSS, a blockchain-based access control system. We reinterpreted the rights of access and employed more lightweight encryption algorithms to protect privacy because of the nature of CPSS big data. in [12] explores this problem and proposes a blockchain-

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

based IoT network access control mechanism, making the case for switching from the conventional centralised IoT-server architecture to a decentralised one. A safe platform for device registration is established by utilising smart contracts in conjunction with the blockchain. [13] considered the ownership, use, and protection of rights and incorporated blockchain technology into the administration and protection of digital music copyrights. The author incorporated blockchain technology into the administration and protection of digital music copyrights, considering the ownership, use, and protection of rights. The findings support the advancement and use of blockchain technology and deep learning techniques in the digital music industry. [14] proposes a permissioned blockchain architecture that incorporates support vector Machine (SVM) for real-time autonomous and distributed UAV service monitoring, aiming to ensure SLA enforcement and trust. We provide a permissioned blockchain architecture that takes Support Vector Machine (SVM) into account for real-time autonomous and distributed UAV service monitoring in order to fulfil the SLA enforcement and trust model. [15] aims to address cloud security concerns by examining the architectural differences between various cloud architectures and investigating methods based on deep learning, blockchain, and cryptography. In order to solve cloud security concerns, this study examines the architectural differences between various cloud architectures and investigates methods based on deep learning, blockchain, and cryptography. [16] uses a deep learning-based multi-task cascaded convolutional neural network (MTCNN) for face detection. The suggested model includes asymmetric encryption standards, blockchain technology, and multi-factor authentication to guarantee the security elements needed in a voting system and provide voters with a hassle-free voting experience. [17] implemented the combined techniques of blockchain and machine learning to protect system transactions and handle a dataset to combat false datasets, addressing the issues outlined above. In order to protect system transactions and handle a dataset to combat false datasets, we implemented the combined techniques of blockchain and machine learning to address the issues outlined above. They applied big data management and analysis techniques to the gathered dataset. [18] proposes a blockchain-based privacy-preserving system for medical data sharing between medical institutions and data users, leveraging searchable encryption and K-anonymity. We specifically use the Hyperledger Fabric Consortium blockchain to enable data users to look up encrypted medical records. in [19] proposes the creation of an intrusion detection system that monitors the safe routing of transactions using a Fully Decentralised Generative Adversarial Network (FDGAN). By creating an intrusion detection system, the suggested system monitors the safe routing of transactions using a Fully Decentralised Generative Adversarial Network (FDGAN). in [20] proposes a blockchain-based approach to safeguarding the datasets created by IoT devices for e-health applications. In order to safeguard the datasets created by IoT devices for e-health applications, we have suggested a blockchain-based approach. In the suggested blockchain-based system, we utilize a private cloud to address the aforementioned problem. [21] provides a comprehensive analysis of blockchain, machine learning, and emerging IoT technologies for their potential applications in healthcare. This paper offers a thorough analysis of blockchain, machine learning, and developing IoT technologies for use in healthcare applications. The reviewed papers comprise an extensive collection of research publications in the fields of machine learning, blockchain, and IoT published on the Web of Science. in [22] Researchers utilize the following metrics to compare these algorithms: recall, accuracy, precision, F1 score, and classification time.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

Based on all performance criteria utilised in the research, with the exception of time, the results show that the Random Forest and AdaBoost classifiers produce extremely similar results and are regarded as the top classifiers. [23] offers methodology for a more extensive spectrum of security qualities for the smart public transport system, as confirmed by comparison with other similar systems. [24] proposes a procedure that focuses on text analysis techniques to enhance the emergency response process of the authorities and filter information using automatically obtained data. In order to support the relief efforts, this procedure focuses on text analysis techniques to enhance the emergency response process of the authorities and filter information utilising automatically obtained data. [25] proposes a recommendation model that aims to assist trainers in making informed decisions about a trainee's future food and exercise regimen. The recommendation model seeks to make it easier for a trainer to make wise selections about a trainee's food and exercise regimen in the future. Finally, we have accessed the system performance in terms of latency, throughput, resource utilisation, and altering ordered and peer nodes using Hyperledger Calliper for performance study. [26] provides a thorough analysis of the four ways that blockchain can help AI in this study. In this study, we provide a thorough analysis of these four ways that blockchain can help AI. Our analysis of 27 English-language articles released in 2018 and 2021 uncovers both potential and obstacles for further research. [27] employed LSTM's pure propagation malicious code detection technology, which enhanced security by collaborating with an artificial intelligence consensus process. The methodology employed LSTM's pure propagation malicious code detection technology, which enhanced security by collaborating with an artificial intelligence consensus process. Furthermore, Unity ML built a virtual world with the beta version as part of an experiment. [28] aims to reduce each MD's long-term system expenses, including latency, energy use, and smart contract fees, through this Optimisation challenge. The goal of this Optimisation challenge is to reduce each MD's long-term system expenses, including latency, energy use, and smart contract fees. We use a double-duelling Q-network to construct an enhanced deep reinforcement learning system to handle the proposed offloading problem. [29] integrates blockchain, edge computing, and machine learning technologies into the suggested smart manufacturing system for this procedure. For this procedure, the suggested smart manufacturing system integrates blockchain, edge computing, and machine learning technologies. In a similar vein, edge computing balances the computational burden and gives the devices prompt responses. In [30], there is the possibility of combining blockchain technology with hashing to achieve a higher level of threat mitigation through the suggested approach without the requirement of complex encryption. The study's main contribution is the demonstration that it is possible to combine blockchain technology with hashing to provide a greater level of threat mitigation via the suggested approach, all without the need for complex encryption.

III. Methodology

A novel approach to enhancing the access control mechanism for Internet of Things (IoT) is presented, leveraging blockchain technology and encryption to establish a robust and secure information service platform. The proposed framework involves encrypting medical data before storing it in a distributed cloud infrastructure. Identity-based broadcast encryption is employed, alongside the integration of an incentive mechanism to motivate customers and miners in

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

sustaining the platform[18,19]. The key management scheme is centred around an advanced dynamic contributory broadcast encryption-based method, incorporating a newly devised Proof of Work (PoW) blockchain consensus mechanism as foundational components. Additionally, the system ensures data recoverability through the application of blockchain technology. Figure 1 present the proposed model of access control approach.

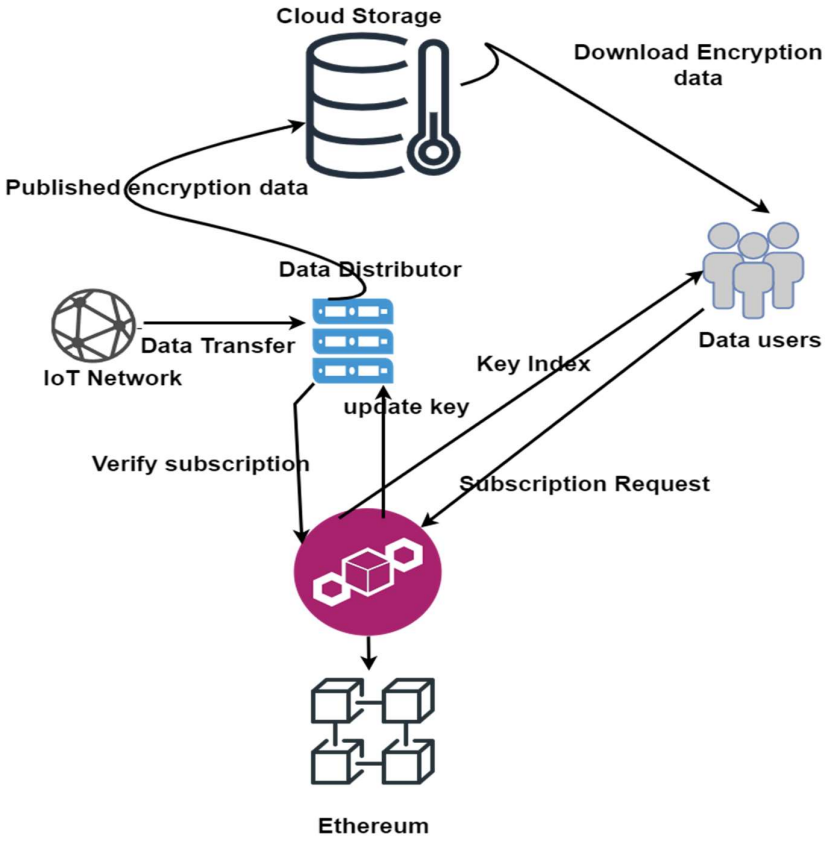

Figure 1 Proposed Model of Access Control Key Approach Based on Blockchain Technology

The access control approach encompasses five fundamental pillars: the IoT network, data distributor, data users, cloud storage, and blockchain technology, all contributing to a comprehensive key management system. These entities are interconnected through a series of arrows symbolizing the flow of information. The algorithmic processing of this access control mechanism is detailed as follows:

IoT Network: The foundation of the access control approach lies in the IoT network. This network serves as the primary interface for connecting various IoT devices and sensors.

Data Distributor: The data distributor plays a crucial role in the process, facilitating the efficient and secure distribution of data. It acts as an intermediary between the IoT network and the subsequent stages of data processing.

Data Users: Entities or users requiring access to the data are represented in this pillar. These can include individuals, applications, or devices authorized to retrieve and interact with the information.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

Cloud Storage: Encrypted data is stored in distributed cloud storage, ensuring accessibility and scalability. The cloud storage acts as a secure repository for the sensitive information.
Blockchain Technology: The backbone of the key management system is blockchain technology. It provides a decentralized and tamper-resistant ledger for recording key transactions and access permissions. The proposed framework leverages blockchain to enhance security and transparency.
The interconnections among these pillars are visualized through arrows, depicting the flow of data and control between different components of the access control mechanism. The processing of algorithm describes below.
Implementing access control in the Internet of Things (IoT) using blockchain involves ensuring secure and tamper-resistant permission management. Below is a simplified algorithmic overview for access control in IoT leveraging blockchain:
Node Registration and Key Generation:
Node Identity: Each IoT device registers on the network and generates a public-private key pair. The public key is used as the device's unique identifier.
Blockchain Initialization:
Smart Contracts:
Deploy smart contracts on the blockchain to manage access permissions. Define contract functions for adding, modifying, and revoking access rights.
Access Control List (ACL) Creation:
Access Rules:
Define access control rules specifying which devices or entities can interact with specific IoT devices.
Store these rules in the form of ACLs on the blockchain.
Access Request:
Permission Query:
When an entity (e.g., another IoT device, user, or application) seeks access to a device, it sends a request to the blockchain.
Access Verification:
Smart contracts on the blockchain execute the access request, verifying if the requesting entity's public key matches the allowed keys in the ACL.
Additional conditions, such as time restrictions or transaction history, may be checked.
Consensus Validation:
The blockchain network validates the transaction using the chosen consensus mechanism to achieve agreement on the access decision.
Immutable Record:
Successful access requests and modifications to ACLs are recorded as transactions on the blockchain, creating an immutable and transparent history.
Key Updates:
Implement mechanisms for dynamic key exchange if access permissions need to be updated regularly. Smart contracts can facilitate the secure exchange of updated keys.
Transaction History:
Maintain an audit trail of access-related transactions for accountability and forensic purposes.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

This helps in investigating any security incidents or disputes.

Self-Sovereign Identity:

Explore decentralized identity solutions to give entities control over their identities and enhance privacy.

Key Revocation:

Include a mechanism for revoking access, such as removing a device's public key from the ACL in case of compromise or authorization change.

IV. Experimental analysis

The implementation of the system utilizes the Ethereum blockchain, a public blockchain renowned for its support of smart contracts. The smart contract responsible for executing the data access control mechanism is developed using the Remix Integrated Development Environment (IDE) and subsequently deployed on the Ethereum public test network Goerli through the Metamask software. Written in Solidity, the primary programming language for Ethereum smart contracts. To facilitate an illustrative experimental evaluation, a comparative analysis of Ethereum gas consumption is conducted, focusing on the distribution of keys in the proposed model. The model incorporates encrypted keys stored in the smart contract as the bytes32 data type. For effective management of access privileges, including the granting or revocation of access to off-chain published content, interaction with the smart contract is imperative. This interaction results in the modification of the smart contract storage to reflect the changes in access control[28,29,30].

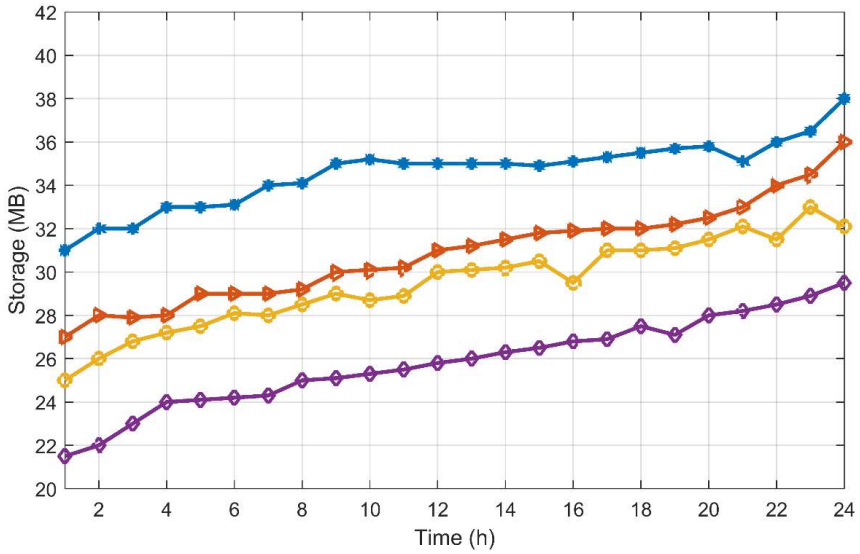

Figure: 2 Performance analysis of storage (MB) and time (h) during the process of transaction.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

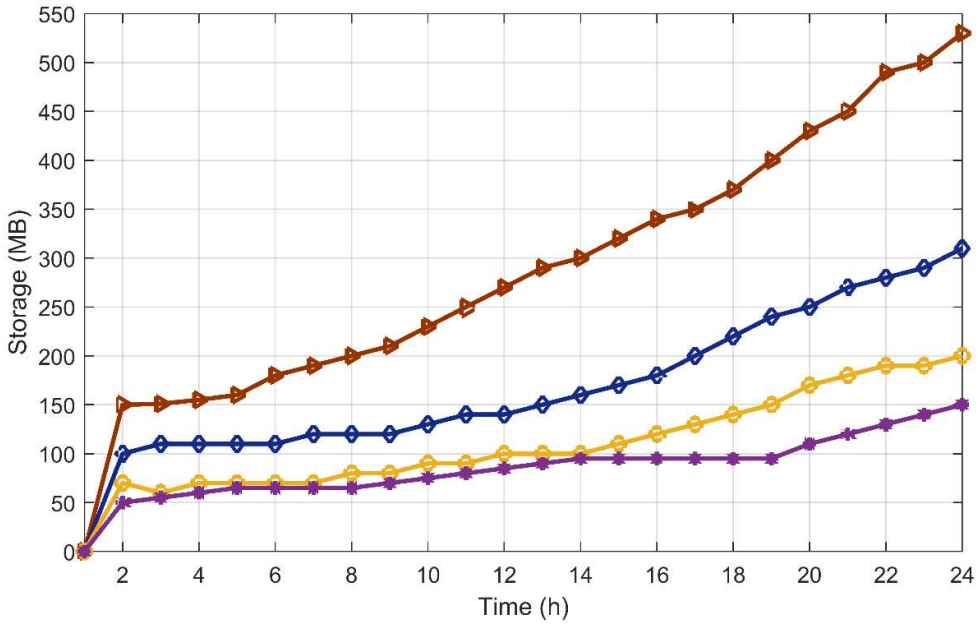

Figure: 3 Performance analysis of storage (MB) and time (h) for different access approach of key.

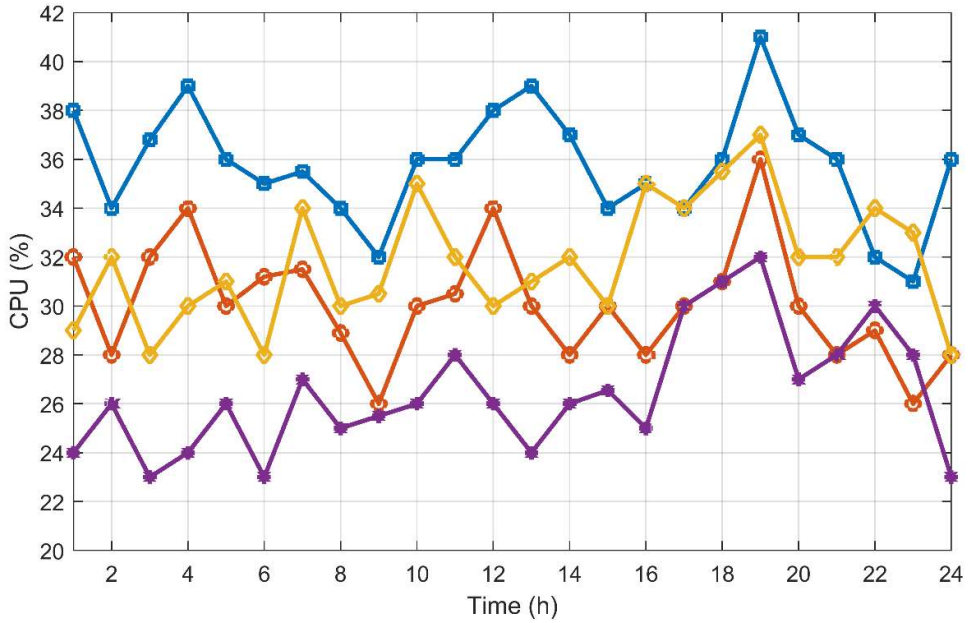

Figure: 4 Performance analysis of CPU utilization (%) and time (h) for access approach of blockchain.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

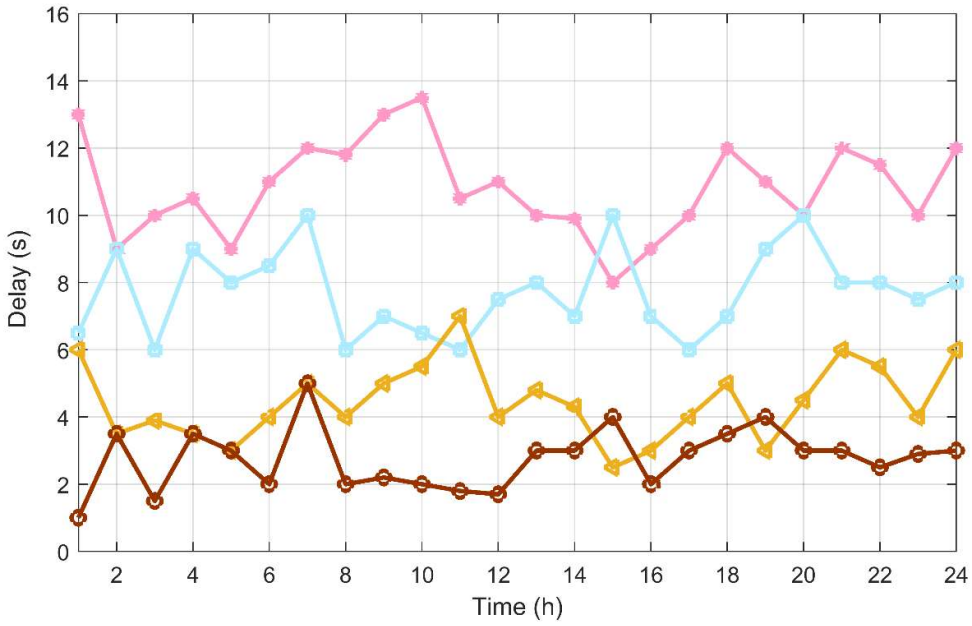

Figure: 5 Performance analysis of Delay (s) and time (h) for updated key index of blockchain in IoT network.

V. Conclusion & Future Work

The integration of blockchain technology and a distributed Internet of Things (IoT) platform is the central focus of this article. The motivation behind this work stems from the imperative need to devise a solution that ensures the confidentiality, integrity, and access control of transmitted data within the IoT network. Crucially, this solution aims to achieve these goals without relying on a central authority and without deeming the IoT platform itself as inherently trustworthy. Addressing the potential bottleneck posed by the requirement for a trusted authority to release access permissions, and recognizing the vulnerability of policies to tampering and violations, the article introduces permissioned blockchains. These blockchains enable the management of transactions without necessitating trust in the IoT platform and without the imposition of centralization. Consequently, the distributed IoT platform assumes the responsibility for blockchain management, resulting in a significant advantage. To validate the proposed solution, a practical test-bed comprising four prototypes of Network Operating Systems (NOSs) has been employed. The chosen architecture for testing purposes reflects a real-world scenario. Performance indices such as computing effort, storage overhead, and latency have undergone evaluation, affirming the viability and effectiveness of the designed solution.

References

[1]. Dwivedi, Ashutosh Dhar, Rajani Singh, Keshav Kaushik, Raghava Rao Mukkamala, and Waleed S. Alnumay. "Blockchain and AI for 5G-enabled IoT: Challenges, Opportunities and Solutions."

[2]. Wu, Tong, Weijie Wang, Chuan Zhang, Weiting Zhang, Liehuang Zhu, Keke Gai, and Haotian Wang. "Blockchain-Based Anonymous Data Sharing With Accountability for Internet of Things." IEEE Internet of Things Journal 10, no. 6 (2022): 5461-5475.

[3]. Oktian, Yustus Eko, and Sang-Gon Lee. "Borderchain: Blockchain-based access control framework for the internet of things endpoint." IEEE Access 9 (2020): 3592-3615.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

[4]. Rizzardi, Alessandra, Sabrina Sicari, Daniele Miorandi, and Alberto Coen-Porisini. "Securing the access control policies to the Internet of Things resources through permissioned blockchain." Concurrency and Computation: Practice and Experience 34, no. 15 (2022): e6934.

[5]. Khan, Muhammad Adnan, Sagheer Abbas, Abdur Rehman, Yousaf Saeed, Asim Zeb, M. Irfan Uddin, Nidal Nasser, and Asmaa Ali. "A machine learning approach for blockchain-based smart home networks security." IEEE Network 35, no. 3 (2020): 223-229.

[6]. Abdulrazzaq, Sazeen Taha, Farooq Safauldeen Omar, and Maral A. Mustafa. "Decentralized security and data integrity of blockchain using deep learning techniques." Periodicals of Engineering and Natural Sciences 8, no. 3 (2020): 1911-1923.

[7]. Abbas, Khizar, Muhammad Afaq, Talha Ahmed Khan, and Wang-Cheol Song. "A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry." Electronics 9, no. 5 (2020): 852.

[8]. Abdi, Adam Ibrahim, Fathy Elbouraey Eassa, Kamal Jambi, Khalid Almarhabi, and Abdullah Saad Al-Malaise Al-Ghamdi. "Blockchain platforms and access control classification for IoT systems." Symmetry 12, no. 10 (2020): 1663.

[9]. Zhang, Zhizhao, Tianzhi Yang, and Yuan Liu. "SABlockFL: a blockchain-based smart agent system architecture and its application in federated learning." International Journal of Crowd Science 4, no. 2 (2020): 133-147.

[10]. Khan, Prince Waqas, Yung-Cheol Byun, and Namje Park. "IoT-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning." Sensors 20, no. 10 (2020): 2990.

[11]. Tan, Liang, Na Shi, Caixia Yang, and Keping Yu. "A blockchain-based access control framework for cyber-physical-social system big data." IEEE Access 8 (2020): 77215-77226.

[12]. Javaid, Uzair, Furqan Jameel, Umair Javaid, Muhammad Toaha Raza Khan, and Riku Jäntti. "Rogue device mitigation in the internet of things: a blockchain-based access control approach." Mobile Information Systems 2020 (2020): 1-13.

[13]. Li, Huizi. "Piano automatic computer composition by deep learning and blockchain technology." IEEE Access 8 (2020): 188951-188958.

[14]. Khan, Amjad Saeed, Gaojie Chen, Yogachandran Rahulamathavan, Gan Zheng, Basil Assadhan, and Sangarapillai Lambotharan. "Trusted UAV network coverage using blockchain, machine learning, and auction mechanisms." IEEE Access 8 (2020): 118219-118234.

[15]. Andi, Hari Krishnan. "Estimating the Role of Blockchain, Deep Learning and Cryptography algorithms in Cloud Security." Journal of Trends in Computer Science and Smart Technology 3, no. 4 (2021): 305-313.

[16]. Pooja, S., Laiju K. Raju, and Utkarsh Chhapekar. "Face detection using deep learning to ensure a coercion resistant blockchain-based electronic voting." Engineered Science 16 (2021): 341-353.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

[17]. Shahbazi, Zeinab, and Yung-Cheol Byun. "Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing." Sensors 21, no. 4 (2021): 1467.

[18]. Chen, Yingwen, Linghang Meng, Huan Zhou, and Guangtao Xue. "A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection." Wireless Communications and Mobile Computing 2021 (2021): 1-12.

[19]. Rajasoundaran, S., SVN Santhosh Kumar, Munuswamy Selvi, Sannasi Ganapathy, R. Rakesh, and Arupathraj Kannan. "Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks." Wireless Networks 27, no. 7 (2021): 4513-4534.

[20]. Gadekallu, Thippa Reddy, M. K. Manoj, Neeraj Kumar, Saqib Hakak, and Sweta Bhattacharya. "Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications." IEEE Internet of Things Magazine 4, no. 3 (2021): 30-33.

[21]. Imran, Muhammad, Umar Zaman, Imran, Junaid Imtiaz, Muhammad Fayaz, and Jeonghwan Gwak. "Comprehensive survey of iot, machine learning, and blockchain for health care applications: A topical assessment for pandemic preparedness, challenges, and solutions." Electronics 10, no. 20 (2021): 2501.

[22]. Shahin, Rawan, and Khair Eddin Sabri. "A secure IoT framework based on blockchain and machine learning." International Journal of Computing and Digital System (2021).

[23]. Liu, Tong, Fariza Sabrina, Julian Jang-Jaccard, Wen Xu, and Yuanyuan Wei. "Artificial intelligence-enabled DDoS detection for blockchain-based smart transport systems." Sensors 22, no. 1 (2021): 32.

[24]. Shahbazi, Zeinab, and Yung-Cheol Byun. "Blockchain-based event detection and trust verification using natural language processing and machine learning." IEEE Access 10 (2021): 5790-5800.

[25]. Jamil, Faisal, Hyun Kook Kahng, Suyeon Kim, and Do-Hyeun Kim. "Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms." Sensors 21, no. 5 (2021): 1640.

[26]. Wang, Ruonan, Min Luo, Yihong Wen, Lianhai Wang, Kim-Kwang Raymond Choo, and Debiao He. "The applications of blockchain in artificial intelligence." Security and Communication Networks 2021 (2021): 1-16.

[27]. Kim, Seong-Kyu. "Automotive vulnerability analysis for deep learning blockchain consensus algorithm." Electronics 11, no. 1 (2021): 119.

[28]. Nguyen, Dinh C., Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. "Secure computation offloading in blockchain based IoT networks with deep reinforcement learning." IEEE Transactions on Network Science and Engineering 8, no. 4 (2021): 3192-3208.

[29]. Shahbazi, Zeinab, and Yung-Cheol Byun. "Improving transactional data system based on an edge computing–blockchain–machine learning integrated framework." Processes 9, no. 1 (2021): 92.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

[30]. Reddy, S. Sai Satyanarayana. "Joint Framework for Access Control and Authentication using Blockchain over Cloud Environment." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12, no. 14 (2021): 4750-4760.