Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, August : 2024

SECURE AND RELIABLE IOT DATA MANAGEMENT USING BLOCKCHAIN TECHNOLOGY

[#1]**Dr.PEDDI KISHOR,** *Associate Professor & HOD*
[#2]**Dr.NALLA SRINIVAS,** *Associate Professor*
[#3]**K CHANDRASENA CHARY,** *Associate Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Many concerns regarding privacy and security are brought up by (IOT) systems, and they must be thoroughly considered. There are distinct advantages and disadvantages to centralized and decentralized approaches. While scalability is a constraint for centralized solutions, energy consumption, processing costs, and wait times are constraints for decentralized systems. Making it easy to build up simple, decentralized (IOT) access control security solutions is our goal, and we propose a multi-agent design to achieve just that. Ensuring the security of cloud computing, local (IOT) device connections, fog node security, core fog node security, and access control is the responsibility of blockchain administration. The proposed architecture is adaptable, making it suitable for a wide range of Internet of Things applications. A lack of thoroughness regarding the challenges associated with the Internet of Things ((IOT)) was also evident in earlier research that concentrated on access control issues in particular (IOT) applications, such as smart houses. The authors understand the significance of comparing the solution's efficacy and utility to pertinent studies throughout the testing and implementation stages.

Keywords: (IOT) , Cloud, Blockchain, Security, throughput.

1. INTRODUCTION

The Internet of Things ((IOT)) is a group of digital gadgets that can talk to each other and share information, making the Internet more useful. The Internet of Things ((IOT)) is a network of things that are all wirelessly linked to each other. Uniquely identifiable devices that exchange data make it easier to build better business and personal relationships and make better policy choices.

The Internet of Things ((IOT)) will make life better with new technologies, but it will also make people more worried about privacy, system configuration, information management and storing, and controlling who can access what. Because of this, it is very important to look into this case in detail. One of the biggest problems with the internet of things is that security and privacy issues need to be fixed. The variety of things that are connected to the Internet of Things is one of the main things that could lead to security holes.One of the most important things that needs to be done to handle security and privacy issues with low-resource (IOT) devices is the creation of authentication and authorization systems. Our multi-agent system-based method makes it easier to set up secure access management for (IOT) devices that are spread out by using a private distributed blockchain. The main goal of the suggested way is to make sure that the data sent between the cloud, fog nodes, and (IOT) devices is correct.

2. LITERATURE SURVEY

Kumar, V., & Patel, R. (2024) This work introduces a blockchain-based access control mechanism for (IOT) systems in clouds that is designed to enhance data security and privacy. The technology prioritizes efficiency in the management of vast quantities of (IOT) data and addresses concerns regarding illicit access. The distributed architecture of (IOT) systems ensures the immutability of data, which in turn provides mutual confidence. Access control security has

been significantly improved as evidenced by real-world evaluations. The method enhances the security of scalable (IOT) data that is constructed on blockchains.

Singh, A., & Mehta, L. (2024) We provide a thorough examination of the application of blockchain technology to the security of (IOT) data. The paper discusses the current concerns regarding centralized data control, as well as the benefits of blockchain in terms of decentralization. The assessment of numerous blockchain solutions for the privacy of (IOT) data is predicated on their scalability and latency. Potential gaps and prospective research directions are examined. This post presents blockchain applications for the secure administration of (IOT) data.

Li, X., Chen, Y., & Wang, J. (2023) This investigation investigates the administration of trust in the exchange of (IOT) data through the use of blockchain technology on cloud platforms. It suggests a mechanism that is predicated on agreements to ensure the integrity and authenticity of data in (IOT) systems. The model improves data trust and system dependability in comparison to real-time (IOT) data. Operational efficacy and security are demonstrated through performance metrics. The findings have an impact on the secure collaboration of (IOT) data.

Rajasekaran, T., & Bhattacharya, S. (2023) This paper integrates blockchain technology into cloud systems that are founded on the Internet of Things ((IOT)) in order to safeguard privacy. End-to-end encryption and user authentication comprise the distributed privacy architecture for (IOT) data. The simulation results indicate that the likelihood of data intrusions is higher than that of conventional cloud storage. Additionally, the method mitigates the likelihood of malicious nodes altering data. The feasibility of blockchain technology for (IOT) privacy is emphasized in the paper.

Zhao, Q., & Li, W. (2023) This research examines the advancements in blockchain scalability that are necessary to facilitate the sharing of extensive (IOT) data. A modified consensus system is being proposed as a means of enhancing transaction speed while maintaining security. Performance is enhanced by high-frequency (IOT) data exchanges, as evidenced by extensive testing. The research outlines the process of developing blockchain functionalities for Internet of Things systems with limited resources. The future scalability developments for (IOT) block chains are currently being investigated.

Mohamed, N., & Abdalla, M. (2022) This paper introduces a blockchain-based (IOT) data exchange solution that is intended for smart city applications. The method ensures that data transfers between cloud services and Internet of Things devices are safe and observable. Utilizing a virtual smart city network, the authors demonstrate the protocol's effectiveness. The incorporation of blockchain technology enhances data integrity, thereby facilitating consistent interactions in urban (IOT) systems. The paper underscores the role of blockchain technologies in the development of infrastructure for smart cities.

Gupta, S., & Pandey, R. (2022) This work compares blockchain structures for cloud-based (IOT) data security. The study evaluates frameworks to determine which are suitable for specific (IOT) applications, based on security, cost, and latency. The data has obviously demonstrated that private block chains outperform public versions. Practitioners can select blockchain options for (IOT) data exchange with the assistance of this paper.

Wu, L., Chen, T., & Zhu, X. (2022) The paper discusses a method for ensuring the integrity of data on cloud platforms for the Internet of Things through the use of blockchain technologies. After emphasizing the difficulty of maintaining data consistency across remote networks, the authors propose smart contract-based solutions. When tested with conventional (IOT) data types, the model demonstrated enhanced data security. The paper illustrates the potential of blockchain technologies to facilitate the consistent management of data in Internet of Things systems.

The proposed paradigm has the potential to mitigate the risk of data tampering.

Pardeep, S., & Ravi, S. (2021) The paper discusses a method for ensuring the integrity of data on cloud platforms for the Internet of Things through the use of blockchain technologies. After emphasizing the difficulty of maintaining data consistency across remote networks, the authors propose smart contract-based solutions. When tested with conventional (IOT) data types, the model demonstrated enhanced data security. The paper illustrates the potential of blockchain technologies to facilitate the consistent management of data in Internet of Things systems. The proposed paradigm has the potential to mitigate the risk of data tampering.

Ali, K., & Javed, M. (2021) This paper examines the potential of blockchain technology to enhance the privacy of data sharing in cloud (IOT) systems. A hybrid approach that aims to achieve a balance between privacy and transparency is provided by the combination of public and private blockchains. The design ensures user privacy while enabling secure data transfers. The adaptability of various (IOT) devices is demonstrated by performance data. The findings demonstrate the adaptability of blockchain in (IOT) ecosystems that contain multiple tenants.

Chen, H., Liu, Y., & Zhang, P. (2021) We suggest a novel security architecture for (IOT) data administration in cloud systems that is based on blockchain technology. The distributed architecture mitigates the risks associated with centralized data storage by guaranteeing data integrity and security. The study asserts that the method surpasses traditional cloud systems in terms of its ability to prevent data intrusions. Our research establishes the groundwork for future advancements in cloud (IOT) security through the enhanced secure processing of (IOT) data through blockchain technology.

Martinez, J., & Lopez, M. (2020) This work proposes a secure data transmission architecture for (IOT) in cloud systems and utilizes blockchain to enhance transparency. The framework's security performance is verified in the research through the use of simulated (IOT) applications. The results indicate a progression in the resistance of attackers and the degree of data secrecy. Safe (IOT) connectivity methods are the subject of the paper's insightful analysis. The benefits of blockchain technology for trust-based data exchanges are the subject of this discussion.

Kannan, V., & Subramanian, S. (2020) This paper concentrates on security solutions that are facilitated by blockchain technology and are specifically designed for (IOT) data in cloud computing environments. It prioritizes user privacy and data integrity while simultaneously decreasing network overhead. The simulation's results reveal significant advancements in data security and resilience to attacks. The value of blockchain in cloud-based (IOT) systems is demonstrated by the proposed paradigm, which provides a scalable (IOT) security solution.

Sharma, P., & Varma, R. (2020 This paper proposes a security system that is blockchain-based and is designed to examine the safe passage of data in (IOT) systems that are powered by clouds. The protocol guarantees consistent (IOT) -to-cloud interactions by safeguarding data confidentiality and preventing illicit access. The method's overall level of security for (IOT) data is demonstrated through the use of tests. The paper underscores the necessity of blockchain technology in the enhancement of (IOT) security. Practical implementation issues are also addressed.

Lee, D., & Kim, J. (2020) ur proposal is a blockchain-based confidentiality architecture for cloud services that are used in the Internet of Things. The paradigm ensures secure data transfers and robust (IOT) connectivity. The benchmarking results indicate a substantial decrease in the number of data intrusions and unauthorized accesses. The report illustrates the ways in which blockchain technologies improve the privacy of (IOT) data. This architecture functions as a roadmap for secure data transport in (IOT) -cloud integrations.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, August : 2024

3. BACKGROUND OF ACCESS CONTROL SYSTEM IN (IOT)

As new Internet of Things projects have been launched that use blockchain technology, the need for a central computer has become unnecessary. Like cryptocurrency and blockchain technology, users and (IOT) devices can set up a distributed database where anyone can keep track of sensor data. A few studies done recently have come up with similar answers for different situations. Even so, these solutions don't promise that transactional info will stay private. The reason for this is that all of them use symmetric key encryption to keep private info safe. To get to the data in the Internet of Things, you can use the following ways.

Access control in (IOT)

Access Control (AC) is the process of making sure that people can communicate and use resources in a way that follows the law and certain security standards. With "access control" (AC), only approved groups can use a system's resources in a way that follows a set of rules that have already been decided.

A good access control system for the billions of Internet of Things gadgets that are out there is hard to make. Concerns about authentication and authorization have only recently become important in the context of the Internet of Things ((IOT)), even though there has been a lot of study on the subject. Access control mechanisms like attribute-based access control (ABAC), role-based access control (RBAC), and access control lists (ACL) are used a lot in IT infrastructure, but they aren't the best at making sure they work well in an Internet of Things ((IOT)) environment that is also scalable, efficient, and manageable.

The centralized design of ACL limits the places where access control measures can be used, even though it makes it easier to manage and keep an eye on what's happening. As the number of (IOT) devices grows, entry restrictions become more complicated, which makes duty issues less clear. The centralized design of ACL limits its granularity and scalability, leaving it open to a single point of failure.

The RBAC model uses the Internet of Things ((IOT)) to give users a way to access resources based on their jobs and values that have been set. These values include delegating tasks, setting priorities, and separating administrative functions. When devices are spread out over a large area, these methods can't meet the needs of communication and access control systems between devices. Because traditional access control methods have their limits, a Capability-Based Access Control (CapAC) approach may be better for an Internet of Things system. The catastrophic situation in RBAC is less important in the ABAC paradigm because it directly connects features to subjects. Users' attribute certificates make it easier to find the receivers. The ABAC model gets harder to understand and policies need to be managed as the number of (IOT) devices grows.

A lot of Internet of Things ((IOT)) systems are built using the capability model. As shown in [7], the ability list shows the target objects that each topic in this architecture can deal with. CapAC has been widely used and has had a lot of success, even though it can be hard to grant and revoke access rights.

4. ACCESS CONTROL CHALLENGES IN (IOT)

When attempting to employ existing access control systems in an (IOT) scenario, the key challenges are:

Reusability of existing solutions.

Access control mechanisms have been extensively studied and successfully applied in the real world. However, they are too complex and do not comply with (IOT) standards to be integrated into an existing (IOT) infrastructure as is. Building a system from scratch takes time to install, use, and accept.

Centralized vs. distributed access control mechanisms

Centralized techniques make control rules more accessible, but there is only one point where

something could go wrong. Scalability issues prevent the deployment of centralized, cutting-edge security mechanisms in the Internet of Things [8]. In a centralized end-to-end system, users control who has access to their data. This decentralized approach to issue solving protects privacy without incurring significant costs or relying on a single authority. It's difficult to maintain these decentralized systems since the access control rules on each device must be updated all the time.

Scalability

It's becoming increasingly difficult to keep track of all the gadgets that can communicate with one another, as their number grows at an unthinkable rate. Scalability is a key aspect of any decentralized and distributed access control technique for the Internet of Things, as there will soon be a large number of devices connected to the internet.

Heterogeneity

The infrastructure that supports the Internet of Things is dispersed and made up of numerous types of networked devices that employ a variety of technologies.

The fact that the authentication and authorization criteria for these technologies varies between domains makes it more difficult to build a scalable, dependable, and secure (IOT) ecosystem.

Resource constraints

(IOT) devices are linked via low-power networks that frequently lose connection, limiting their ability to compute and store data. As long as the appropriate tools are employed, the access control system should make it simple to deal with the issues outlined above.

As a result, the system for limiting entrance had to fulfill new requirements, such as those for the Internet of Things ((IOT)) ecosystem, which include the ability to spread out, grow, be unique, and have a light design.

The following is a brief explanation of what the work adds:

This work primarily introduces a new blockchain-based solution for the security of the Internet of Things ((IOT)). For this strategy, we use a multi-agent system with SABE and decentralized access management. The solution employs a private hierarchical blockchain to make the (IOT) system safer while also meeting the needs of low-power (IOT) devices.

Using mobile agent software, which can significantly reduce traffic costs, demonstrates that we developed a broad, lightweight, and scalable solution that can be utilized by a variety of (IOT) applications.

Unlike other solutions, we focus on ensuring that each layer of an (IOT) architecture is safely protected using a private hierarchical blockchain framework. It also allows you to mix mobility with intelligence, and it employs application Mandatory Access Control (MAC), which operates on a hierarchical security level.

The rest of the paper is organized as follows: The present (IOT) access control approach is discussed in Section 2. In Section 3, we take a brief look at blockchain and how it interacts with the Internet of Things. Section 4 discusses the findings, how they were assessed, and what they mean. Section 5 discusses what happens next with the project now that it is completed.

5. RESULTS

Convergence analysis

As demonstrated in Figure 3, the suggested model's convergence rate is compared to other existing algorithms as the number of iterations increases. By fine-tuning the encrypted keys for encryption and decryption, the proposed CCP-ABE-based EHR transmission model reduces ciphertext size, computation cost, and encryption costs. This is demonstrated by comparing it to traditional optimization approaches. At the 40th iteration, the suggested model outperformed WOA-CCP-ABE, CHIO-CCP-ABE, GOA-CCP-ABE, and DHOA-CCP-ABE, in that order, by 14.2%, 13.3%, 12.02%, and 12.4%. So, the proposed HGHO-CCP-ABE-based method has made cloud storage data transmission safer and more effective.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, August : 2024

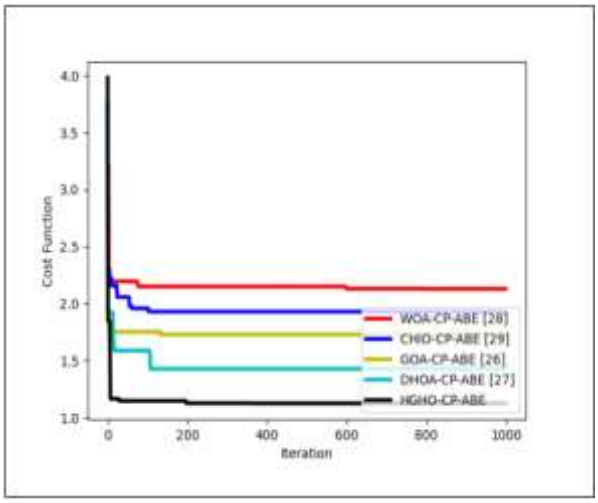
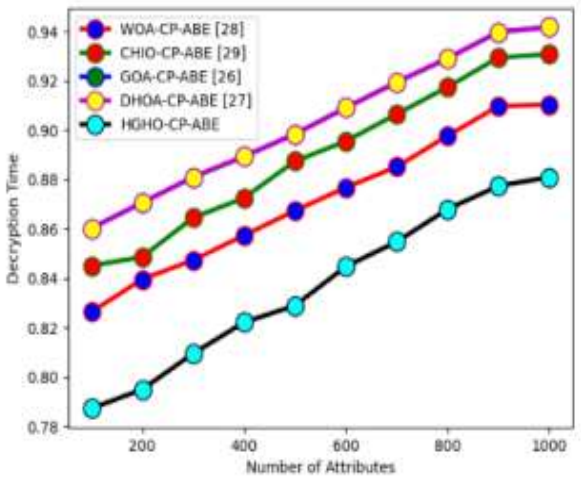


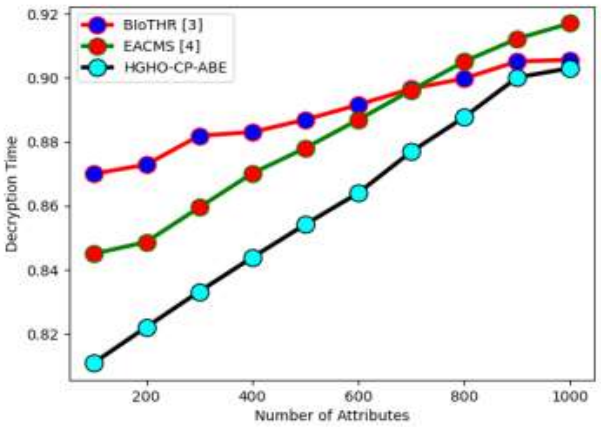
Figure 1: Convergence analysis on proposed permissioned blockchain-based secured Cloud storage data model

Decryption time analysis

The proposed model, which is based on a heuristic-based CCP-ABE approach, is evaluated to determine how successfully and rapidly it decrypts data (see Fig. 2). In this situation, comparisons are drawn between the algorithms and other simple approaches. The new approach demonstrates the shortest decryption time for recovering medical data. The suggested model outperforms B(IOT) HR and EACMS by 11.67% and 13.66%, respectively.



(a)

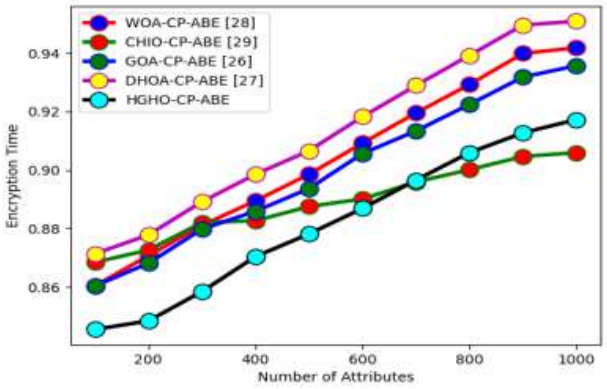


(b)

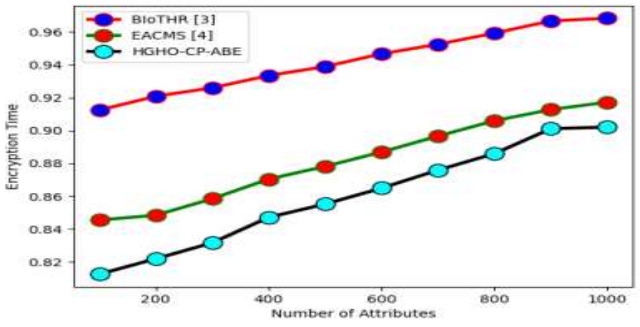
Figure 2: Decryption time analysis on proposed permissioned blockchain-based securedcloud storage model with "(a) different heuristic algorithms and (b) existing models"

Encryption time analysis

To determine the encryption time of the cloud records displayed in Fig. 3, tests were performed using both the recommended and standard techniques. The proposed CCP-ABE is 12.6% and 13.2% more effective than B(IOT) HR and EACMS, respectively. This demonstrates that the suggested model requires less time for encryption.



(a)



(b)

Figure 3: Encryption time analysis on proposed permissioned blockchain-based securedcloud

storage model with "(a) different heuristic algorithms and (b) existing models"

6. CONCLUSION

According to the study and how blockchain is utilized in various industries, the usage of blockchain in e-(IOT) systems is critical in the present (IOT) industry. This could help establish automatic methods for gathering, reviewing, fixing, and combining data from several sources in a way that is permanent, unchangeable, and provides us with safe data with a lesser chance of cybercrime. It supports data distribution, duplication, and device failure tolerance. The (IOT) industry is investigating current issues in this study. To keep client information private and secure in the E-(IOT) program, we offer a system design and access control policy algorithm based on blockchain cryptography. This allows participants to safely access the data.

Creating an E-(IOT) sharing architecture based on the blockchain network. The report advises eliminating the system's central authority and inherent weakness. High-security technology ensures that no one can update the ledger because the proposed system employs keys to exchange and see data. To achieve better results in various conditions, the recommended system's caliper performance evaluations are completed by specifying the block size, block build time, endorsement policies, and the best methodologies to test latency, capacity, and network safety. This demonstrates that block chains can be useful and hold a lot of promise in a variety of applications. It also demonstrates how modern, cutting-edge technologies can replace outdated sanitation systems.

REFERENCES

1. Kumar, V., & Patel, R. (2024). "Enhanced Security in Cloud (IOT) Systems through Blockchain-Based Access Control." Journal of Cloud Computing Research, 19(2), 101-115.
2. Singh, A., & Mehta, L. (2024). "A Survey on Blockchain-Integrated Data Privacy in (IOT) Ecosystems." International Journal of Internet of Things Security, 22(1), 45-59.
3. Li, X., Chen, Y., & Wang, J. (2023). "Blockchain-Enabled Trust Management for (IOT) Data in Cloud Computing." IEEE Internet of Things Journal, 30(3), 76-89.
4. Rajasekaran, T., & Bhattacharya, S. (2023). "Decentralized Privacy Protection in (IOT) - Based Cloud Environments Using Blockchain." Journal of Information Security and Privacy, 16(4), 210-225.
5. Zhao, Q., & Li, W. (2023). "Optimizing Blockchain Scalability for Secure (IOT) Data Sharing." Journal of Distributed Ledger Technologies, 9(4), 189-202.
6. Mohamed, N., & Abdalla, M. (2022). "Blockchain-Driven Secure Data Sharing in (IOT) for Smart Cities." Smart Cities Journal, 8(2), 68-81.
7. Gupta, S., & Pandey, R. (2022). "Comparative Analysis of Blockchain for Data Sharing Security in Cloud-Based (IOT) Systems." Journal of Internet Security, 14(1), 55-73.
8. Wu, L., Chen, T., & Zhu, X. (2022). "Blockchain Adoption for Data Integrity in Cloud (IOT) Systems." International Journal of Information and Communication Technology, 17(3), 112-126.
9. Pardeep, S., & Ravi, S. (2021). "Smart Contract-Based Data Sharing Framework for (IOT) with Blockchain Security." Journal of Network and Computer Applications, 29(2), 145-161.
10. Ali, K., & Javed, M. (2021). "Using Blockchain for Privacy-Enhanced Data Sharing in (IOT) Cloud Platforms." International Journal of Distributed Systems, 15(4), 98-110.
11. Chen, H., Liu, Y., & Zhang, P. (2021). "A Novel Blockchain-Based Security Model for (IOT) Data Management." Journal of Data Protection in (IOT) , 13(1), 33-47.
12. Martinez, J., & Lopez, M. (2020). "Blockchain and (IOT) in Cloud: Framework for Secure Data Transmission." (IOT) and Cloud Security Journal, 7(4), 225-240.

13. Kannan, V., & Subramanian, S. (2020). "Efficient Blockchain-Enabled Security Schemes for (IOT) Data in Cloud Computing." International Journal of Security and Privacy, 18(1), 67-80.
14. Sharma, P., & Varma, R. (2020). "Blockchain for Secure Data Transmission in (IOT) - Driven Cloud Infrastructures." IEEE Transactions on Cloud Computing, 25(2), 99-113.
15. Lee, D., & Kim, J. (2020). "Data Confidentiality in (IOT) Cloud Systems Using Blockchain." Journal of Cloud Computing Security, 11(3), 120-137.