A

Seminar Report

On

NOVEL AND SECURE BLOCKCHAIN FRAMEWORK FOR HEALTH APPLICATIONS IN IOT

Submitted in partial fulfillment for award of the degree of

Bachelor of Technology

In

Computer Science and Engineering

By

Mukund Maheshwari (2060005)

Under the Guidance of

Mr. Aviral Awasthi

ASSISTANT PROFESSOR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING GRAPHIC ERA HILL UNIVERSITY, BHIMTAL CAMPUS

SATTAL ROAD, P.O. BHOWALI,

DISTRICT- NAINITAL-263132

2023-2024

STUDENT'S DECLARATION

I, **Mukund Maheshwari,** hereby declare the work, which is being presented in the report, entitled "**Novel and Secure blockchain framework for health applications In IOT"** in partial fulfillment of the requirement for the award of the degree **Bachelor of Technology (B.Tech.)** in the session **2023-2024**, is an authentic record of my work carried out under the supervision of **Mr. Aviral Awasthi.**

The matter embodied in this report has not been submitted by me for the award of any other degree.

Date:10 June 2024

Mukund Maheshwari

(2060005)

CERTIFICATE

The seminar report entitled **Novel and Secure blockchain framework for health applications in IOT** being submitted by **Mukund Maheshwari** of B.Tech.(CSE) to Graphic Era Hill University Bhimtal Campus for the award of bonafide work carried out by him. She has worked under my guidance and supervision and fulfilled the requirement for the submission of a report.

Mr. Aviral Awasthi	**Dr. Ankur Bist**
(Seminar Coordinator)	**(HOD, CSE)**

ACKNOWLEDGEMENT

I take immense pleasure in thanking the Honorable Director **‘Prof. (Col.) Anil Nair (Retd.)’,** GEHU Bhimtal Campus to permit me and carry out this report work with his excellent and optimistic supervision. This has all been possible due to his novel inspiration, able guidance, and useful suggestions that helped me to develop as a creative researcher and complete the research work, in time.

Words are inadequate in offering my thanks to GOD for providing me with everything that I need. I again want to extend thanks to our president **‘Prof. (Dr.) Kamal Ghanshala’** for providing me with all infrastructure and facilities to work in need without which this work could not be possible.

Many thanks to **‘Dr. Ankur Singh Bisht’**(Head, Department of Computer Science and Engineering, GEHU Bhimtal Campus), & **‘Mr. Aviral Awasthi’** (Assistant Professor, Department of Computer Science and Engineering, GEHU Bhimtal Campus), our seminar coordinator and other faculties for their insightful comments, constructive suggestions, valuable advice, and time in reviewing this thesis.

Finally, yet importantly, I would like to express my heartiest thanks to my beloved parents,for their moral support, affection, and blessings. I would also like to pay my sincere thanks to all my friends and well-wishers for their help and wishes for the successful completion of this research.

Mukund Maheshwari, 206005

ABSTRACT

The Internet of Things (IoT) has experienced significant growth over the past decade, introducing several challenges for the continuous operation of IoT applications. These challenges include resource constraints, central server overload, and the risk of unauthorized use of private data. Concurrently, Blockchain technology has gained popularity, particularly in cryptocurrencies, offering critical features such as consensus mechanisms, peer-to-peer communications, trust-building without a third party, and transaction control via smart contracts. This study proposes an innovative IoT-Blockchain integration architecture using Ethereum Blockchain within a rich-thin client IoT approach. This architecture addresses IoT resource limitations by distributing the load between devices: limited-resource devices act as thin-clients, while higher-resource devices function as rich-clients. Both types of clients can access the blockchain and collect data, but only rich-clients perform the mining process. To demonstrate the architecture's effectiveness, we implement a healthcare system for surgical process management and compare its performance against other IoT-based blockchain architectures. Our results indicate that the proposed architecture effectively mitigates the challenges posed by IoT device limitations, making it suitable for a wide range of IoT applications..

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

The twenty-first century has witnessed rapid advancements across various technological domains, profoundly impacting nearly every facet of human life. Today, technology plays an integral role in our daily personal and professional activities, exemplified by the proliferation of smart devices like phones and tablets, which monitor health metrics such as distance traveled, heart rate, and calorie expenditure. This convergence of sensors and communication devices has given rise to the concept of the Internet of Things (IoT), wherein interconnected devices interact, share data, and make decisions autonomously.

IoT, first coined by Kevin Ashton in 1999, has emerged as a significant domain within the realm of networking, facilitating a plethora of applications across diverse fields of life. From enabling smart homes to fostering the development of smart cities, IoT has revolutionized the way we interact with and utilize technology. However, this exponential growth in IoT adoption has also brought forth a myriad of challenges and issues that necessitate urgent attention and resolution.

One of the primary challenges facing IoT is the inherent limitations of IoT devices, characterized by low computing power, limited storage capacity, and constrained network bandwidth. Additionally, the prevalent use of centralized system architectures in IoT exacerbates challenges related to cost, scalability, server failures, and security vulnerabilities.

Despite the remarkable advancements facilitated by IoT, concerns persist regarding data privacy, security, and trust within centralized architectures, such as those employed in cloud computing. This lack of trust stems from the opaque nature of data handling and utilization, wherein end-users have limited visibility into the usage and manipulation of their generated data.

In response to these challenges, researchers have explored integrating Blockchain technology with IoT to address issues of privacy, security, and resource constraints. Blockchain, initially introduced in 2008 through the invention of Bitcoin by Satoshi Nakamoto, offers a decentralized, immutable ledger system that ensures data integrity and transparency. The integration of Blockchain with IoT holds promise in revolutionizing IoT applications by providing a secure and trustless environment for data exchange and management.

However, integrating Blockchain with IoT poses several challenges, including computational limitations of IoT devices, storage constraints, overhead traffic, and scalability issues inherent in Blockchain networks. Overcoming these challenges requires innovative solutions and robust integration architectures tailored to the unique requirements of IoT applications.

This study endeavors to address the limitations and challenges associated with integrating Blockchain and IoT, with a particular focus on healthcare applications. Leveraging previous research efforts, we aim to enhance integration architectures to effectively mitigate resource constraints at the IoT layer and streamline implementation at the Blockchain layer. By testing our integration framework in the healthcare domain, we seek to demonstrate its efficacy in addressing security, privacy, and resource limitations, thereby unlocking new possibilities for IoT applications in healthcare management

CHAPTER 2: BLOCKCHAIN AND IOT INTEGRATION

The integration of Blockchain with IoT, termed as BCoT, addresses the inherent challenges of IoT systems, including fragmentation, low interoperability, resource limitations, and privacy vulnerabilities. By leveraging Blockchain technology, BCoT offers enhanced interoperability, stability, and trustworthiness to IoT systems, thereby unlocking new possibilities for seamless interaction and data management.

Advantages of Blockchain Integration:

1. **Enhanced Interoperability:** Blockchain integration facilitates the transformation and storage of heterogeneous IoT data, enabling seamless communication across decentralized networks.
2. **Improved Stability:** Blockchain secures IoT data through cryptographic encryption, ensuring data integrity and protection against security breaches. Additionally, automatic device configuration upgrades enhance system security.
3. **Data Traceability and Trustworthiness:** Blockchain ensures the traceability and authenticity of IoT data, allowing for transparent verification of transactions. Blockchain-based traceability frameworks enhance trust in data integrity.
4. **Autonomous Communications:** Blockchain enables automated interactions within IoT systems, streamlining data exchange and decision-making processes.

Integration Architectures:

BCoT integration architectures vary based on factors such as IoT device interactions and connectivity requirements. Three primary integration approaches include:

- **Blockchain as a Database:** Utilizes Blockchain for storing IoT data selectively, improving reliability and security, particularly in low-latency IoT interactions.
- **Blockchain in All Layers:** Directs all interactions through Blockchain, ensuring a tamper-proof history of transactions and enhancing data traceability and flexibility. However, this approach may incur increased bandwidth and record-keeping overhead.
- **Hybrid Approach:** Combines Blockchain and IoT interactions selectively, leveraging fog and cloud computing to overcome scalability and resource constraints.

Blockchain Schemes for IoT:

Several Blockchain frameworks, such as Ethereum, Hyperledger, Multichain, Litecoin, Lisk, and Quorum, offer diverse solutions for integrating Blockchain with IoT. These frameworks provide varying levels of functionality, consensus mechanisms, and security features, catering to different IoT application requirements

CHAPTER 3: METHODOLOGIES

This study introduces an Enhanced Rich-Thin-Client architecture (ERTCA) to address the limitations of IoT devices. The proposed architecture makes two main contributions:

a) **Resource Optimization**: To prevent the overload and potential crash of IoT nodes, a solution is provided to allocate tasks efficiently to each node based on its resources.

b) **Improved Connectivity**: To enhance the connection between IoT and Blockchain platforms, the Blockchain is connected to a major node with high capabilities, allowing other nodes to benefit from Blockchain without being overloaded. Node classification is based on computational power and storage capability.

These contributions address some of the issues faced by other integration methods, such as resource limitations at the IoT layer and implementation difficulties at the Blockchain layer. Building upon previous work, this study refines the integration architecture to more effectively address resource limitations.

A. ERTCA

The ERTCA integrates Ethereum Blockchain with a rich-thin-client IoT solution. It aims to achieve the research goals by addressing the limitations of IoT and the centralized architecture problem. The architecture includes thin clients responsible for user interface and data collection, and rich clients capable of processing and storing data similar to personal computers. The Ethereum private Blockchain network is used as the base Blockchain system. Smart contracts are utilized for relatively complex connections between different IoT devices and users. Unlike previous work, this study introduces a second-level thin client solely responsible for collecting data without interacting with the system, reducing complexity in each layer of the architecture.

System Architecture and Topology

The Enhanced Rich-Thin-Clients Architecture (ERTCA) differs from hierarchical architecture by distributing tasks among all clients rather than duplicating tasks across levels. It employs a star topology, where thin clients are connected to specific rich clients, ensuring decentralized processing and fault tolerance. Each rich client includes an Ethereum Blockchain node, facilitating peer-to-peer communication. The topology ensures robustness against failures, crucial for real-time monitoring in critical applications.

Privacy and Security

The architecture ensures client anonymity and data integrity through Ethereum's account system and Blockchain authentication mechanisms. Each client is assigned a unique Ethereum account, providing anonymity and preventing unauthorized access. IoT devices are protected from attacks, and illegitimate transactions are rejected by the Blockchain.

B. Application Scenario

The proposed architecture is applicable to various domains, including healthcare. A scenario inspired by real-world hospital protocols is presented, focusing on surgical process management. The scenario outlines preoperative, intraoperative, and postoperative stages, highlighting the critical need for real-time monitoring and rapid response in surgical environments.

C. Implementation of ERTCA-Based Surgery Management System

A private Ethereum network serves as the underlying Blockchain system for the application. Smart contracts are deployed to manage the surgical process, reflecting real-life procedures. The system architecture includes thin clients responsible for patient data collection and rich clients managing the surgical process. ReactJS is used to create the graphical user interface, while Web3.js facilitates interaction with the Blockchain. MetaMask provides a user interface for account interaction.

D. Smart Contract Implementation to SMS

Smart contracts are implemented using Solidity to maintain the surgery management process. The contract includes a database, event handlers, and functions to manage patient records and surgical events. Patient information adheres to global Electronic Health Record (EHR) standards, ensuring compatibility and interoperability with existing healthcare systems. Blockchain ensures data reliability, security, and immutability.

CHAPTER 4: RESULT AND DISCUSSIONS

In this chapter, we evaluate the main components of the system: the proposed architecture and the customized Blockchain. First, we assess the performance of ERTCA and compare it with a hierarchical architecture. Then, we evaluate the efficiency of the customized private Ethereum-based Blockchain.

A. ERTCA Evaluation

The primary objective of this work is to establish an architecture capable of integrating IoT and Blockchain while addressing the resource limitations of IoT devices. The proposed ERTCA framework aims to distribute the workload effectively to enable IoT devices to handle Blockchain operations. To evaluate its performance, we compare it with a hierarchical architecture.

In the hierarchical architecture, each system is treated as a layer, with each layer having its miners and smart contracts. This approach lacks differentiation between rich and thin clients, as all clients are Blockchain full nodes with their smart contract definitions.

The performance evaluation reveals that ERTCA outperforms the hierarchical architecture. While the hierarchical architecture exhibits high peaks in CPU and network performance across all systems, ERTCA's peaks are primarily in rich clients' device performance. Additionally, ERTCA demonstrates superior efficiency, consuming significantly less time and resources compared to the hierarchical architecture.

B. Private Ethereum-based Blockchain Evaluation

The performance of the customized private Ethereum-based Blockchain is evaluated using Ganache Test Net, an environment similar to the main Public Ethereum network but without associated financial costs. Smart contracts are tested for their execution time and gas usage.

The mining time in Ganache Test Net is found to be significantly lower than in the main Public Ethereum network, which incurs high costs. Smart contracts in the private Ethereum network demonstrate efficient execution, with a full cycle of the surgery management process consuming only 5 seconds. Gas usage is within the set limits, indicating efficient execution of smart contracts by miners.

C. Discussion

The results indicate that the integration of IoT and Blockchain can be optimized through efficient architecture design. ERTCA provides a solution to the resource limitations of IoT devices by distributing tasks according to device capabilities. This optimization enhances performance and ensures reliable data transmission while maintaining privacy and security.

The findings suggest that ERTCA can be effectively implemented in IoT applications with numerous attached devices and stakeholders. For example, in a smart school application, thin clients can represent students, while rich clients manage educational processes and second-level thin clients handle educational devices.

CHAPTER 5: CONCLUSION

Healthcare management is a critical aspect of society, continuously evolving with advancements in technology. While numerous systems and applications exist for health monitoring, fostering end-user adoption and usage remains a challenge. This research introduces a collaborative healthcare management system leveraging IoT and Blockchain integration through the ERTCA architecture. By exemplifying the usability of this technology, the system aims to enhance performance, resource utilization, data privacy, and security.

The integration of Blockchain technology, whether in private infrastructures or public networks like Ethereum, offers several benefits. However, the financial costs associated with the Ethereum Public network can escalate with high transaction volumes, highlighting the importance of considering performance, privacy, and security when opting for private Blockchain systems.

In conclusion, the integration of Blockchain and IoT presents an opportunity to develop collaborative health monitoring systems, ensuring data immutability and preserving business logic while potentially introducing gamification elements to encourage user engagement. Future directions for research include expanding tests and evaluations of ERTCA with other IoT-Blockchain integration architectures, studying its scalability and security, evaluating Smart Contracts on different Blockchains, and exploring application scenarios beyond healthcare management. While extending the system to include aspects like medication management and medical consultation data, the focus remains on leveraging technology to enhance healthcare processes and outcomes

REFERENCES

1. K. Ashton, ‘‘That ’Internet of Things’ thing,’’ RFID J., vol. 22, no. 7, pp. 97–114, 2009.
2. L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, ‘‘Blockchain for managing heterogeneous Internet of Things: A perspective architec ture
3. Litecoin Wiki Contributors, Litecoin Wiki. (May 8, 2019). Main Page. Accessed: Jan. 1, 2022.
4. A. Dorri, S. S. Kanhere, and R. Jurdak, ‘‘Towards an optimized BlockChain for IoT,’’ in Proc. 2nd Int. Conf. Internet Things Design Implement., Apr. 2017
5. R. Kaluri, D. S. Rajput, Q. Xin, K. Lakshmanna, S. Bhattacharya, T. R. Gadekallu, and P. K. R. Maddikunta, ‘‘Roughsets-based approach for predicting battery life in IoT,’
6. R. Sujatha, C. Navaneethan, R. Kaluri, and S. Prasanna, ‘‘Optimized digital transformation in government services with blockchain,’’ in Blockchain Technology and Applications. Boca Raton, FL, USA: Auerbach Publications, 2020
7. https://ieeexplore.ieee.org/Xplore