Islamic University of Technology (IUT)
Department of Computer Science and Engineering (CSE)

IoT Devices Authentication using Blockchain Technology

Authors
Kone Awa Nadege - 180041142
Halima Housseini - 180041143
Ubada Abbas Bao Ibrahim - 180041145

Supervisor
Dr. Md. Moniruzzaman
Assistant Professor, Department of CSE

Co-Supervisor
Imtiaj Ahmed Chowdhury
Lecturer, Department of CSE

A thesis submitted to the Department of CSE in partial fulfillment of the requirements for the degree of B.Sc. Engineering in CSE
Academic Year: 2021 - 2022
May 25, 2023

Declaration of Authorship

This is to declare that the research presented in this thesis is the outcome of the analysis and experiments carried out by Kone Awa Nadege, Halima Housseini, and Ubada Abbas Bao Ibrahim under the supervision of Dr. Md. Moniruzzaman, Assistant Professor, Department of Computer Science and Engineering (CSE), Islamic University of Technology (IUT), Dhaka, Bangladesh. It is also declared that neither this thesis nor any part of this thesis has been submitted anywhere else for any degree or diploma. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

Authors:

Kone

Kone Awa Nadege
Student ID - 180041142

Halima Housseini
Student ID - 180041143

عبادة

Ubada Abbas Bao Ibrahim
Student ID - 180041145

Supervisor:

Dr. Md. Moniruzzaman
Assistant Professor
Department of Computer Science and Engineering
Islamic University of Technology (IUT)

Co-supervisor:

27.05.23

Imtiaj Ahmed Chowdhury
Lecturer
Department of Computer Science and Engineering
Islamic University of Technology (IUT)

Acknowledgement

We thank the Almighty Allah for making us able to complete our thesis without any major challenges.

We are also thankful to our parents for motivating and encouraging us to fulfill our dreams and wishes.

We would like to express our grateful appreciation for **Dr. Md. Moniruzzaman**, Assistant Professor, Department of Computer Science & Engineering, IUT for being our supervisor and mentor. His motivation, suggestions, and insights for this research have been fruitful. His valuable opinion, time, and input were provided throughout the thesis work, from the first phase of thesis topics, and modifications, until the project implementation and finalization which helped us to do our thesis work in an efficient manner.

We are also grateful to **Imtiaj Ahmed Chowdhury**, Lecturer, Department of Computer Science & Engineering, IUT for his valuable inspection and suggestions on our proposal.

Abstract

The Internet of Things (IoT) has brought revolution the way we live and work, but with this revolution it has also brought new security challenges. IoT devices often lack strong authentication mechanisms, making them vulnerable to cyber-attacks or malicious intents. Blockchain technology has come up as a prospective solution to this problem, offering a secure and decentralized way to authenticate IoT devices.

In this paper, we propose a novel approach to IoT authentication using blockchain technology. Our approach leverages the decentralized properties of blockchain technology to provide secure and reliable authentication for IoT devices. We discuss the challenges of implementing blockchain-based IoT authentication, such as scalability and privacy, and propose solutions to address these challenges. we tend to propose a blockchain primarily based authentication theme named Bubbles of Trust. wherever solely devices settled within a selected bubble will be sure and attested with.

We also present a proof-of-concept implementation of our approach authentication process, demonstrating how blockchain-based authentication can be used to securely authorize and validate transactions between IoT devices. Our implementation uses a combination of cryptographic techniques, such as digital signatures and public-key cryptography, to ensure the integrity and authenticity of transactions.

Overall, our approach offers a promising solution to the security challenges of IoT devices in matters of security. It provides a secure and decentralized authentication mechanism that can help prevent unauthorized access or communication and protect sensitive data.

Index Items: IoT devices, Security, Authentication, Blockchain, Ethereum

Contents

1 Introduction

1.1 Overview

Our paper proposes an improved model which can be applied to Internet of Things (IoT) networks, which are characterized by devices that can interact with each other and with their environment in a social and collaborative manner (bubbles).

With the rapid growth of IoT devices, the need for a trustworthy and secure network has become increasingly important. IoT devices have a limited amount of processing power and storage space, so traditional authentication mechanisms like login and password combinations are not appropriate. As a result, it can be difficult to use encryption and securely store passwords, making these devices vulnerable to hacking and breaches of security... Therefore, a new approach to trust is necessary to effectively manage the interactions among devices in IoT networks. The "Bubbles of Trust" model proposed in the paper provides a new methodology for establishing trust in IoT devices. The model considers the social relationships and interactions among devices to form "bubbles" of trusted devices. It is feasible to create a safe chain of trust across devices, facilitating secure communication and transactions, by utilizing the immutable and decentralized features of blockchain. With no requirement for a server or other centralized authority to oversee the authentication process, it is now feasible to authenticate devices in the Internet of Things.

1.1.1 Blockchain Technology

Blockchain technology is a distributed ledger that stores information in a decentralized and immutable manner. The information stored on the blockchain is verified and secured using cryptographic techniques, which make it virtually impossible to alter or hack. This makes blockchain technology an ideal candidate for authentication and verification purposes. It is a very significant solution to varies sectors including tech, finance and supply chain management etc.

In the context of IoT authentication, blockchain technology can provide a secure and decentralized way to authenticate IoT devices. By leveraging the cryptographic properties of blockchain technology, IoT devices can be authenticated in a way that is tamper-proof, transparent, and reliable. This can help prevent unauthorized access and protect sensitive data in IoT networks.

By using blockchain technology, cryptocurrency transactions can be securely authorized and validated, making them less susceptible to fraud and hacking.

Overall, the use of blockchain technology in IoT authentication and cryptocurrency transactions has significant potential to improve the security and reliability of these systems. Its ability to provide secure and tamper-proof authentication and verification makes it a valuable tool in the increasingly complex and interconnected world of IoT and cryptocurrency. There are generally three main types of blockchain networks that we considered using for this thesis: public, private, and consortium.
Public blockchains, such as Bitcoin and Ethereum, are open to anyone and allow

anyone to participate in the network as a node. These networks are typically decentralized and transparent, and anyone can view and access the information on the blockchain.
Private blockchains are used within organizations or between trusted parties, and access to the network is restricted. Private blockchains are typically more centralized than public blockchains, and the nodes are typically controlled by a single entity or group of entities.
Consortium blockchains are a hybrid of public and private blockchains, where a group of organizations controls the network, but it is not open to the public. Consortium blockchains are often used in industries where multiple organizations need to share data and collaborate on a shared network.

The choice of which type of blockchain to use depends on the specific use case and requirements of the project. Each type of blockchain has its own advantages and disadvantages, and the decision of which type to use should be made based on factors such as security, scalability, and access control.

1.1.2 Internet of Things

The Internet of Things (IoT) is a network of physical objects like cars, appliances, and other household things that can collect and share data because they are equipped with sensors, software, and network connectivity. IoT involves the use of internet-connected devices that can interact with one another to exchange data and carry out tasks. For instance, a fitness tracker worn on the wrist can be used to monitor a person's activity levels, and a smart home system can be used to regulate the temperature and lighting in a home.
IoT devices typically involve three main components:

- Sensors and Actuators: These are the physical devices that collect data and perform actions. Examples include temperature sensors, motion detectors, and smart locks.

- Network Connectivity: This is the communication infrastructure that allows devices to connect to the internet and exchange data. This can be achieved through Wi-Fi, cellular, or other network technologies.

- Cloud Computing: This is the central repository where data is stored and processed. The cloud is responsible for analyzing the data collected by IoT devices and making decisions based on that data.

By leveraging the power of blockchain technology and smart contracts, the Bubbles of Trust project could potentially revolutionize the way we interact with IoT devices and share data securely.

1.1.3 Security threats in IoT

The Internet of Things (IoT) is vulnerable to several security threats and the following list includes some of the IoT security issues that we will focus on for the scope of this thesis:

- **Data Breaches:**IoT devices can be vulnerable to hacking and cyber attacks, which can result in sensitive data being stolen or compromised.
- **Unauthorized Access:** IoT devices can be accessed by unauthorized users, allowing them to control or manipulate the device for malicious purposes.
- **Device Tampering:** IoT devices can be physically altered or manipulated, compromising their security and reliability.
- **Malware:** IoT devices can be infected with malware, which can allow attackers to steal data or gain control of the device.
- **Insecure Communication:** IoT devices often use insecure communication protocols, which can leave them vulnerable to hacking and cyber-attacks.

Blockchain technology can provide a secure solution to many of these security threats by offering a decentralized and immutable record of all transactions. For example, blockchain can be used to authenticate IoT devices, ensuring that only authorized devices have access to sensitive information and systems. Blockchain can also be used to secure communication between IoT devices, ensuring that all data exchanged between devices is secure and tamper-proof.

Overall, blockchain technology has the potential to provide a secure and reliable solution for IoT security threats, helping to mitigate the risk of data breaches and cyber attacks, and improving the overall security and reliability of IoT systems.

1.2 Problem Statement

The Bubbles of Trust project addresses the issue of establishing trust relationships between different Internet of Things (IoT) devices and their users in a decentralized and secure manner. With the burgeoning number of connected devices, it becomes ever more crucial to guarantee that users can repose faith in the devices they interact with and the data they share with them. However, current approaches to establishing trust often rely on centralized authorities or third-party intermediaries, which can create security vulnerabilities and limit the scalability of IoT systems. The Bubbles of Trust project aims to address these challenges with the use of the power of blockchain technology and smart contracts to create a secure, decentralized trust framework for IoT devices. The goal is to enable users to easily establish trust relationships between their devices and those of others, without relying on centralized authorities or intermediaries. This would allow for more secure and efficient communication and data sharing between IoT devices, while also ensuring user privacy and control.

Two main issues to address in this paper:
1. Authentication: With the increasing integration of IoT devices into various industries, the secure authentication of these devices has become a crucial concern so we need a system where by using simple and efficient methods, everyone trusts one another.
2. Safe Communication: The secure communication of IoT devices is also a major concern, as it is important to ensure that only authorized devices from existing bubbles can communicate safely.

1.3 Motivation

As computer science engineering students that specialize in Networking with a keen interest in cryptography, We were drawn to the concept of the Blockchain and its potential to transform the way we interact with the world around us. We also delved deeper into the IoT ecosystem, as they are part of our everyday life, we became increasingly aware of the security and privacy challenges associated with the widespread adoption of connected devices. As a result of this, we started searching into the burgeoning area of blockchain technology and its potential uses in safeguarding Internet of Things (IoT) devices.

The idea of using blockchain technology for IoT authentication was particularly intriguing to us, as it offered a novel approach to addressing the security and privacy challenges of the IoT ecosystem. The use of a decentralized and immutable ledger to authenticate and authorize IoT devices provided a promising solution to the challenges of securing the IoT ecosystem, while also enabling new levels of interoperability and scalability.

Moreover, the potential real-world benefits of using blockchain technology for IoT authentication were compelling. The increased security, privacy, and accountability of the IoT ecosystem could enable the development of new applications and services, leading to more efficient and innovative use cases of connected devices.

Overall, the opportunity to work on the IoT Authentication using Blockchain Technology project was a natural fit for our interests and expertise. We were motivated by the potential of the project to contribute to the development of a more secure and trustworthy IoT ecosystem, while also exploring the cutting-edge intersection of blockchain technology and the Internet of Things that we will be able to implement all over African states.

1.4 Research Challenges

Based on our proposed methodology implementation, the research challenges associated with implementing the proposed blockchain-based IoT authentication solution include:

1. Security: While blockchain technology provides strong security guarantees, it is not immune to attacks. The authors highlight the need to consider attack vectors and vulnerabilities specific to IoT devices, such as physical attacks, and develop mitigation strategies to address these threats.

2. Cost: Implementing a blockchain-based IoT authentication solution can be expensive due to the costs associated with storing and processing data on the blockchain network. The authors propose using a hybrid blockchain model that leverages both public and private blockchains to reduce costs while maintaining security and scalability.

3. communication between bubbles: We propose a simulation to show how the limitations of the existing system work to ensure communication between bubbles while preventing man-in-the-middle attacks.

1.5 Thesis Outline

In Chapter 1 we have discussed our study in a precise and concise manner.
Chapter 2 deals with the necessary literature review for our study.
In Chapter 3 we have stated the skeleton of our proposed methodology, and flowchart to provide a detailed insight of the working procedure of our proposed method.
Chapter 4 shows the results and analysis of the successful implementation of our proposed method.
The final segment of this study contains all the references.

2 Literature Review

The literature on IoT authentication and blockchain technology is rapidly evolving, reflecting the growing interest in using blockchain system technology to address the security and privacy challenges of the Internet of Things (IoT) ecosystem. This section provides an overview of the key findings and insights from the existing literature on IoT authentication using traditional authentication systems and using blockchain technology.

2.1 Traditional authentication approach

Traditional authentication approaches have been widely used in securing computer networks and systems for many years. In their paper [10], authors Sharma and Saini (2015) provide a comprehensive review of traditional authentication mechanisms, including password-based authentication, biometric authentication, and token-based authentication. Password-based authentication is one of the most widely used authentication mechanisms. Users are required to enter a username and a password to authenticate themselves. The authors discuss the strengths and weaknesses of password-based authentication, including its simplicity and ease of use, but also its vulnerability to attacks such as password guessing and brute force attacks. Biometric authentication involves using physical characteristics such as fingerprints, iris patterns, and facial recognition to authenticate users. The authors discuss the advantages and limitations of biometric authentication, including its uniqueness and non-repudiation properties, but also its susceptibility to attacks such as spoofing and replay attacks. Token-based authentication involves the use of physical tokens such as smart cards or USB devices to authenticate users. The authors discuss the strengths and weaknesses of token-based authentication, including its high level of security, but also its cost and usability challenges.

Continuous authentication is a crucial aspect of secure device-to-device communication, particularly in the context of the Internet of Things (IoT) where devices interact autonomously. In recent years, there has been an increasing focus on developing lightweight protocols that ensure continuous authentication while minimizing computational and communication overhead. This literature review explores the research work on lightweight continuous authentication protocols for device-to-device communication.

One notable contribution in this field is the paper [23] by Shah et al. (2023) and Syed et al. The authors address the need for efficient and secure continuous authentication in IoT environments where devices communicate directly with each other. They propose a lightweight protocol that minimizes the computational burden on resource-constrained IoT devices while providing robust authentication mechanisms.

The protocol proposed by Shaghaghi et al. (2023) leverages the concept of continuous monitoring and evaluation of device behavior to establish and maintain trust in device-to-device communication. By analyzing various behavioral attributes, such as communication patterns and energy consumption, the protocol can continuously verify the authenticity of devices involved in communication. Moreover, the lightweight nature of the protocol ensures efficient utilization of device resources, making it suitable for resource-constrained IoT environments.

Another important research work in the field of lightweight continuous authentication is The hierarchical architecture presented by Baig et al. (2023) provides an effective solution for managing the computational and communication overhead associated with continuous authentication in large-scale IoT networks. By distributing the authentication tasks among multiple domains, the protocol achieves scalability without compromising security. Furthermore, the lightweight authentication mechanisms employed in each domain ensure minimal resource consumption and latency.

In summary, the research on lightweight continuous authentication protocols for device-to-device communication in IoT environments has seen significant advancements. Baig et al. (2023) proposed a lightweight protocol that focuses on continuous monitoring of device behavior to ensure trust in communication. Baig et al. (2023) addressed scalability challenges by introducing a hierarchical architecture with lightweight authentication mechanisms. These research works contribute to the development of efficient and secure continuous authentication protocols for resource-constrained IoT environments.

This section of the literature review provides an overview of recent advancements in IoT device authentication, with a particular focus on the collaborative PHY-aided technique proposed in [22] which presents an overview of existing IoT device authentication techniques, such as cryptographic approaches, biometric-based methods, and physical layer (PHY)-based techniques. The review highlights the advantages and limitations of each approach, emphasizing the need for robust and efficient end-to-end authentication mechanisms.

The Collaborative PHY-Aided Technique: [22] introduces a novel collaborative PHY-aided technique for end-to-end IoT device authentication. The review discusses the core concepts and methodology employed in the proposed approach. The technique leverages the unique physical characteristics of IoT devices, such as their radio frequency (RF) signatures, to establish secure and reliable device authentication.

Experimental Evaluation: The literature review analyzes the experimental evaluation presented in [22]. It examines the setup, metrics, and results obtained from the experiments conducted to validate the effectiveness and efficiency of the proposed technique. The review discusses the performance improvements achieved by the collaborative PHY-aided technique compared to existing authentication methods.

Comparison with Existing Approaches: This section compares the collaborative PHY-aided technique with other state-of-the-art authentication methods in terms of security, scalability, computational overhead, and resource utilization. The review highlights the unique advantages offered by the proposed technique and identifies potential areas for further improvement.

Discussion and Future Directions: The review provides a critical analysis of the collaborative PHY-aided technique, discussing its strengths, limitations, and potential implications. It also identifies future research directions and open challenges in the field of end-to-end IoT device authentication. The review suggests potential enhancements to the proposed technique, such as exploring machine learning algorithms to improve the accuracy of device identification.

With the increasing complexity of modern network infrastructures and the rise of sophisticated cyber threats, traditional perimeter-based security models have proven inadequate. [21] offers a paradigm shift by adopting a proactive and continuous security approach that challenges the assumption of trust within network environments. Syed et al. provide an in-depth analysis of Zero Trust Architecture (ZTA) in their comprehensive survey, highlighting its importance in contemporary network security strategies.

Background and Concepts: To establish a foundational understanding of ZTA concepts, principles, and core components, Shah et al. discuss the evolution of security models from perimeter-based approaches to the Zero Trust model. They emphasize the shift from implicit trust to explicit verification in access control decisions. The review also explores the key characteristics and architectural principles that underpin ZTA, such as identity-based access control, continuous monitoring, and network segmentation.

Methodology of the Comprehensive Survey: Shahet al. detail their methodology in conducting the comprehensive survey on ZTA. They outline the data collection techniques, research scope, and selection criteria used to identify relevant literature. The review evaluates the rigor and comprehensiveness of the survey's analysis, including the categorization and synthesis of the surveyed works, as presented by the authors.

Key Findings and Contributions: The comprehensive survey by Syed et al. presents several key findings and contributions to the field of ZTA. Their analysis covers various aspects, including ZTA adoption trends, implementation challenges, architectural components, security controls, and evaluation frameworks. The review discusses the insights gained from the survey and their implications for organizations considering ZTA deployment.

Comparative Analysis: The literature review conducts a comparative analysis of the surveyed works, drawing on the comprehensive survey by Syed et al. It identifies common trends, challenges, and best practices in ZTA implementation. The review examines the similarities and differences in the surveyed literature, such as the use of different security controls, integration with existing security frameworks, and scalability considerations, as highlighted by the authors.

Limitations and Future Research Directions: Syed et al. acknowledge certain limitations and propose future research directions in their comprehensive survey. The review critically evaluates these limitations and potential areas for improvement, such as scalability concerns, interoperability with legacy systems, and the need for standardized evaluation methodologies. The review aligns with the authors' proposed future research directions to address these challenges and enhance the effectiveness of ZTA implementation.

In conclusion, the comprehensive survey by Syed et al. provides valuable insights into the state-of-the-art in ZTA research. The literature review highlights the key contributions, methodologies, and findings of the survey, offering a broader understanding of ZTA adoption and its impact on network security. It emphasizes the need for further research and industry-wide collaboration to address the challenges and advance the adoption of ZTA in real-world environments.

In the paper titled [24] the authors propose a novel framework that combines blockchain technology with unified authentication and access control mechanisms to enhance the security of lightweight Internet of Things (IoT) systems operating in mobile communication environments.

The authors start by highlighting the growing prevalence of lightweight IoT devices and the need for robust authentication and access control mechanisms in these systems. They emphasize the challenges posed by the limited resources and mobility of these devices, which require efficient and lightweight security solutions.

The proposed framework leverages blockchain technology to provide a decentralized and tamper-resistant authentication and access control infrastructure. The authors discuss the integration of blockchain into the architecture, enabling the storage and verification of authentication and access control data in a distributed and immutable manner. This enhances the security and integrity of the system by eliminating single points of failure and reducing the vulnerability to unauthorized access.

The unified authentication and access control mechanism in the framework ensures that users and devices are authenticated and authorized consistently across the IoT system. The authors describe how various authentication factors, such as biometrics, credentials, and contextual information, can be utilized to establish the identity and trustworthiness of users and devices. The blockchain-based storage and verification process enable efficient and secure authentication and access control operations.

To evaluate the effectiveness of the proposed framework, the authors conduct experiments and performance evaluations. They assess key metrics such as authentication accuracy, response time, and resource consumption. The results demonstrate the feasibility and efficiency of the unified authentication and access control mechanism, highlighting its potential for future mobile communication-based lightweight IoT systems.

The paper concludes by discussing the advantages of the framework. The integration of blockchain technology ensures the decentralization and immutability of authentication and access control data, enhancing security and trust in the IoT system. The unified approach simplifies the authentication and access control processes, reducing complexity and improving user experience. The authors emphasize the applicability and potential of the framework in various real-world IoT scenarios.

[25] introduces the challenge of authenticating users who have physical access to these devices. Conventional authentication methods are often impractical due to the lack of conventional user interfaces, such as keyboards and mice, on IoT devices. In this context, a virtual sensing technique is proposed to enable secure and intuitive authentication by virtually sensing user interactions.

The virtual sensing technique allows IoT devices to detect user "petting" actions through simple touches lasting approximately 2 seconds. Building on this technique, a secure and intuitive authentication method is developed, comparing the petting operations sensed by the device with those captured by a user wristband. Unlike proximity-based authentication, this method requires physical operations, enhancing its security.

The authentication method adopts straightforward authentication operations, including clicking buttons, twisting rotary knobs, and swiping touchscreens, making it intuitive for users. Notably, it does not necessitate any hardware modifications to IoT devices, making it applicable to commercial off-the-shelf (COTS) devices.

Prototypes are built and extensively evaluated, demonstrating the method's high effectiveness, security, usability, and efficiency. This research presents a promising approach to address the authentication challenge in IoT devices, particularly in smart environments where multiple individuals may interact with the devices.

In summary, traditional authentication approaches such as password-based, biometric-based, and token-based authentication have been widely used in securing computer networks and systems. The literature has extensively reviewed the advantages and limitations of each authentication mechanism, their suitability for different use cases, and their usability challenges.

2.2 Blockchain based authentication approach

Blockchain technology has gained significant attention in recent years due to its potential to enhance security in various applications, including authentication.

One of the main advantages that we chose to follow for using blockchain system technology for IoT authentication is the ability to create a decentralized and secure system without the need for a central authority. Another key benefit of using blockchain technology for IoT authentication is the ability to create an immutable and tamper-proof ledger for recording and verifying transactions. This approach has been explored in several studies, including [3] that provide an overview of the IoT and its security and privacy challenges. They highlight that IoT devices are vulnerable to attacks due to their weak security measures, and the data generated by these devices is often transmitted without proper encryption, posing significant privacy risks. The authors then explain the basics of blockchain technology and its potential use for addressing the security and privacy issues of the IoT. Blockchain technology is a decentralized, distributed ledger that provides a secure and transparent way of recording transactions. The authors highlight the main advantages of blockchain technology, such as decentralization, transparency, and immutability. They also discuss the different types of blockchain, such as public, private, and consortium, and their suitability for IoT applications.

[14], propose a blockchain-based identity authentication framework for IoT devices. The proposed framework aims to address the security issues faced by IoT devices, such as identity theft, data breaches, and denial-of-service attacks. By leveraging the distributed consensus mechanism of blockchain, the authors argue that their proposed framework can establish a secure and reliable identity

authentication mechanism for IoT devices.

the research article, [16] by Muhammad Ali Raza, Zeeshan Ali, and Jong-Hyuk Park proposes a novel and effective solution for the access control and management of IoT devices. The authors have done an excellent job of explaining the basics of blockchain technology and its potential use for IoT security. They have also provided a detailed description of the proposed framework, which demonstrates its feasibility and security benefits. The authors have also evaluated the performance and security of the framework and compared it with other access control and management methods. The paper contributes to the body of literature on blockchain-based solutions for IoT security and provides a solid foundation for further research in this area.

In summary, [14], proposes a blockchain-based identity authentication framework for IoT devices. The proposed framework is similar to previous research in the use of blockchain technology in securing IoT devices, but it has its own unique features and contributions. The proposed framework's security and performance are analyzed in detail, and the authors conclude that it is a secure and reliable solution for identity authentication of IoT devices.

The use of blockchain technology in IoT security has been gaining attention in recent years. In their paper [1], authors Amin et al. (2017) propose a decentralized authentication system for IoT using blockchain technology. The proposed system aims to address the security challenges faced by IoT devices, such as identity theft, data breaches, and denial-of-service attacks. Bubbles-of-Trust an Ethereum-based technique for mutually authenticating IoT devices and gateways, is proposed. It is also a public blockchain implementation that seeks to create safe virtual zones where devices may communicate securely.

In summary, [1] proposes a decentralized authentication system for IoT using blockchain technology. It has its own unique features and contributions. The system's security and performance are analyzed in detail, and the authors conclude that it is a viable solution for securing IoT devices in a decentralized manner.

The paper [13] by Khizar Hameed, Saurabh Garg, Muhammad Bilal Amin, and Byeong Kang presents a novel authentication scheme for IoT systems. The authors propose a decentralized approach that utilizes blockchain technology to address the limitations of traditional centralized authentication schemes.

One significant contribution of this paper is the use of formal verification techniques to ensure the correctness and security of the proposed authentication scheme. By subjecting their scheme to formal verification, the authors enhance the reliability and confidence in the solution. Formal verification offers a rigorous and mathematical approach to validate the correctness of a system or protocol, which is crucial for establishing trust in IoT environments.

The proposed authentication scheme leverages the decentralized and immutable nature of blockchain technology. By utilizing smart contracts and distributed ledgers, the scheme establishes trust among IoT devices without relying on a central authority. This decentralized approach mitigates the risks associated with single points of failure and enhances the resilience of the system.

The paper also provides a comprehensive security analysis of the proposed authentication scheme, evaluating its effectiveness against various attacks, including impersonation, replay, and Sybil attacks. The analysis demonstrates that the scheme offers robust protection against these threats, ensuring the integrity and authenticity of IoT communications.

Furthermore, the authors conduct a performance evaluation of the proposed scheme, assessing its efficiency in terms of authentication latency, communication overhead, and resource utilization. The results indicate that the scheme achieves acceptable performance levels while maintaining the desired level of security.

In a comparative analysis with existing authentication schemes for the IoT, the paper highlights the advantages of their proposed scheme, such as enhanced security, decentralized architecture, and formal verification. This analysis helps in understanding the unique contributions of the proposed scheme and its potential for practical implementation.

In conclusion, the paper by Hameed, Garg, Amin, and Kang presents a formally verified blockchain-based decentralized authentication scheme for the Internet of Things. The scheme addresses the security challenges faced by traditional centralized approaches and offers improved security, resilience against attacks, and efficient performance. The use of formal verification techniques further strengthens the reliability and trustworthiness of the proposed solution.

The paper[2] by Alphand et al. addresses the pressing security challenges faced by IoT systems and proposes an architecture that utilizes blockchain technology to enhance security.

The authors begin by highlighting the security vulnerabilities that arise due to the scale and heterogeneity of IoT devices, emphasizing the need for secure communication, data integrity, and access control. They recognize blockchain technology as a potential solution and propose the IoTChain architecture as an approach to integrate IoT and blockchain for enhanced security.

The IoTChain architecture consists of IoT devices, blockchain nodes, and an IoTChain gateway. The authors explain how IoT devices interact with the gateway to securely communicate and exchange data. Blockchain nodes play a crucial role in validating and storing IoT data, ensuring tamper-proof and transparent data storage. Smart contracts are utilized to automate the execution of predefined rules and policies.

The authors highlight the security mechanisms employed in the IoTChain architecture, including cryptographic techniques for secure communication, data integrity, and access control. They emphasize the importance of these mechanisms in protecting IoT devices from threats such as data manipulation, unauthorized access, and replay attacks.

To evaluate the effectiveness of the IoTChain architecture, the authors conduct a performance evaluation. They measure key metrics such as latency, throughput, and energy consumption, providing an analysis of the results obtained. The trade-offs between security and performance in the IoTChain architecture are discussed.

The paper also compares the IoTChain architecture with existing solutions proposed in the literature. The authors highlight the unique features of IoTChain, such as its decentralized nature, robust security mechanisms, and compatibility with existing IoT devices. They discuss the strengths and weaknesses of alternative approaches, including centralized cloud-based architectures and other blockchain-based solutions.

While the IoTChain architecture shows promise in enhancing IoT security, the authors acknowledge its limitations. They discuss potential challenges in implementing IoTChain in practical IoT environments and suggest future directions for research, including scalability enhancements, interoperability with different blockchain platforms, and integration with emerging technologies like edge computing and artificial intelligence.

In conclusion, the paper presents the IoTChain architecture as a blockchain security solution for IoT systems. It highlights the importance of addressing IoT security challenges and provides insights into the features, advantages, and limitations of the proposed architecture.

In the paper [15] Al Ahmed et al presents a novel authentication protocol that draws inspiration from blockchain technology to address the security challenges in IoT networks.

The author begins by emphasizing the vulnerabilities in IoT networks, particularly concerning authentication. Traditional authentication mechanisms often fall short in providing robust security due to resource constraints and the distributed nature of IoT devices. To overcome these limitations, the author proposes the Authentication-Chains protocol, which leverages blockchain concepts to establish a lightweight and secure authentication scheme.

The Authentication-Chains protocol introduces the concept of "authentication chains" as a means to ensure secure and efficient authentication in IoT networks. These authentication chains consist of a sequence of lightweight cryptographic operations, including one-way hash functions and digital signatures. By incorporating these operations, the protocol achieves secure device authentication without requiring extensive computational resources.

The author explains the key components and steps involved in the Authentication-Chains protocol. This includes the generation and propagation of authentication chains, verification processes, and mechanisms to handle compromised devices. The protocol employs a decentralized and distributed approach, where devices collectively validate the authenticity of other devices in the network.

To validate the effectiveness of the Authentication-Chains protocol, the author conducts experiments and performance evaluations. The evaluation includes metrics such as authentication latency, energy consumption, and scalability. The results demonstrate that the protocol achieves efficient and lightweight authentication while maintaining a high level of security.

Furthermore, the author discusses the advantages of the proposed protocol compared to traditional authentication schemes. The Authentication-Chains protocol offers enhanced security, resilience to attacks, and reduced computational overhead. Its lightweight nature makes it suitable for resource-constrained IoT devices, making it a practical solution for secure authentication in IoT networks.

The paper concludes by highlighting the significance of the Authentication-Chains protocol in addressing the security concerns of IoT networks. It emphasizes the potential for widespread adoption and integration into existing IoT infrastructures.

In the paper [28], Fatimah Hussain Al-Naji and Rachid Zagrouba propose a novel architecture that combines continuous authentication and blockchain technology to enhance the security of Internet of Things (IoT) devices.

The authors begin by highlighting the security challenges faced by IoT systems, particularly the need for robust authentication mechanisms to protect against unauthorized access and potential cyber-attacks. Traditional authentication methods may be insufficient in the dynamic and heterogeneous IoT environment, calling for innovative solutions.

The proposed CAB-IoT architecture addresses these challenges by integrating continuous authentication with blockchain technology. Continuous authentication involves constantly verifying the identity and behavior of users and devices in real-time, ensuring ongoing security. The blockchain component provides a decentralized and tamper-resistant ledger for storing authentication data, enhancing the integrity and transparency of the system.

The authors detail the various components of the CAB-IoT architecture, including the continuous authentication module, the blockchain-based authentication storage, and the decision-making mechanism. They describe how user and device data, such as biometric information and behavior patterns, are collected and analyzed in real-time to ensure continuous authentication. The blockchain stores the authentication records securely, preventing unauthorized modifications and providing an immutable audit trail.

To evaluate the effectiveness of CAB-IoT, the authors conduct experiments and performance evaluations. They assess key metrics such as authentication accuracy, response time, and scalability. The results demonstrate the architecture's ability to provide robust and efficient continuous authentication for IoT devices.

The paper concludes by discussing the advantages of the CAB-IoT architecture. By leveraging blockchain technology, it ensures data integrity, enhances trust, and provides a decentralized authentication mechanism. The continuous authentication approach adds an extra layer of security by monitoring user behavior continuously. The authors highlight the potential of the CAB-IoT architecture to strengthen the security of IoT systems and protect against emerging threats.

To conclude, the CAB-IoT architecture was proposed by Fatimah Hussain Al-Naji and Rachid Zagrouba. The integration of continuous authentication and blockchain technology offers a promising solution to the security challenges faced by IoT systems. The experiments conducted demonstrate the effectiveness and efficiency of the architecture, paving the way for improved authentication mechanisms in the IoT domain.

In summary, the literature review summarizes the paper's proposal of a unified authentication and access control framework for future mobile communication-based lightweight IoT systems using blockchain. The integration of blockchain technology enhances security and decentralization, while the unified approach simplifies the authentication and access control processes. The experiments conducted demonstrate the effectiveness and efficiency of the framework, showcasing its potential for securing lightweight IoT systems in mobile communication environments.

3 Proposed Methodology

The implementation of our authentication system for IoT devices using blockchain technology can be divided into several stages. Here is a proposed methodology:

1. System Design: The first step is to design the overall system architecture, which includes identifying the IoT devices that are already signed in the individual bubbles. so only registered devices part of a specific and unique bubble will be able to register or log in.

2. Blockchain Platform Setup: The next step is to set up the blockchain platform, which involves configuring nodes, setting up the consensus mechanism, and defining the smart contracts. the smart contract will receive the credentials of the already signed members of a bubble for new registration and login purpose.

3. Device On-boarding: The IoT devices that will participate in the network need to be on-boarded onto the blockchain platform. This involves registering the devices on the blockchain platform, which is done by creating an identity for each device and storing it on the blockchain(smart contract).

4. Device Authentication: Once the devices are on-boarded, the authentication process can begin. The authentication process involves validating the identity of each device by checking their digital signatures against their public keys stored on the blockchain. If the bubble-id and the device-id are valid, the device is authenticated and granted access to the platform.

5. Safe between-bubbles Communication: Once the devices are authenticated, access control policies can be enforced. This involves using smart contracts to define access control policies and verifying that the devices have the appropriate permissions to access the resources they are requesting. for example, once the devices request to communicate with a device their request is verified and authenticated then processed.

Finally, the implementation of the system for IoT devices using blockchain technology requires a well-defined methodology that covers system design, blockchain platform setup, device onboarding, device authentication, access control, and network monitoring and management.

3.1 Use Case Scenario

The Internet of Things could be used to track environmental conditions. It has the prospective to have a critical role in identifying the presence of catastrophes caused by nature such as storms, earthquakes, and floods. Intelligent environment Monitoring can also be used to identify and track forest fires in their early stages, predict snowfall in polar regions, predict the likelihood of landslides to avoid incidents, and so on. The warning or alert from such situations has the potential to save many individuals all around the world. It can even warn the humanitarian and rescue crew to locate down and reach the impacted areas as quickly as feasible in order to provide assistance. But let's assume for this scenario, the information from an unauthenticated device sent to the rescue team is a false alert, causing panic and the spread of false information leading to chaos around the world. so the use of an authenticated device with a bubble id which proves that the device can be trusted or from a malicious person, to send a reliable and trusted alert to the rescue team, can ensure better and sure communication.

3.2 Skeleton of Proposed Method

Figure 3.2.1 below shows the basic communication mechanism between devices (bubbles) in the model proposed. As we can see in the picture the bubble B1 or the sender which is already identified and paired with the other bubble or the receiver. They share each others bubble ID and verify it, and after verifying give access to each other. The red box indicates a device which is not identified and trusted and has false bubble id. This device is not part of the bubble and hence can not send message to the B2 bubble.

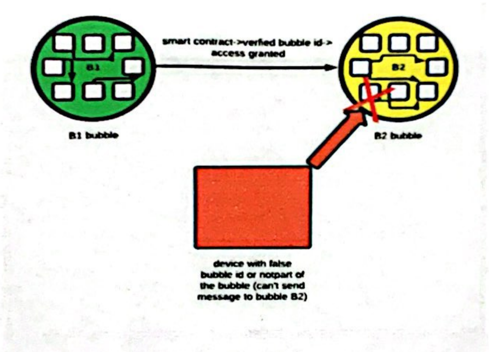

smart contract->verfied bubble id-> access granted
B1
B2
B1 bubble
B2 bubble
device with false bubble id or notpart of the bubble (can't send message to bubble B2)

Figure 3.2.1: basic flowchart of our system

Figure 3.2.2 below shows the basic functionality of the model that we propose on both the back end and front-end. Here in the front end the register page receives the response through the register route and then shows the registration data of the the user. The login page also works the same way. It receives the response and gets back with the login data through login route. The dashboard page in the front end has multiple functionalities, it provides with it's response and receives new messages. It also has options to request device messeages and receive message response.

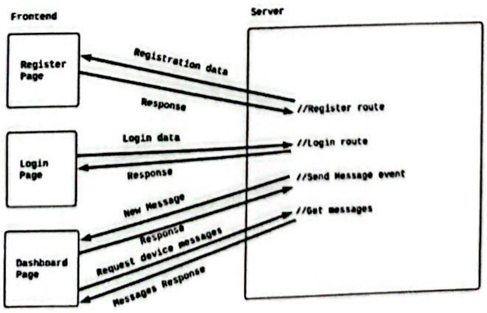
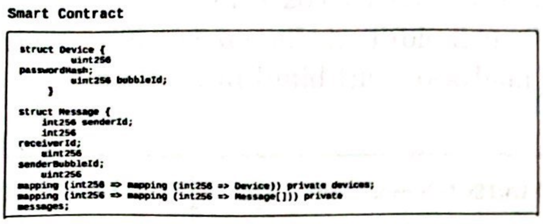


Figure 3.2.2: skeleton of the system

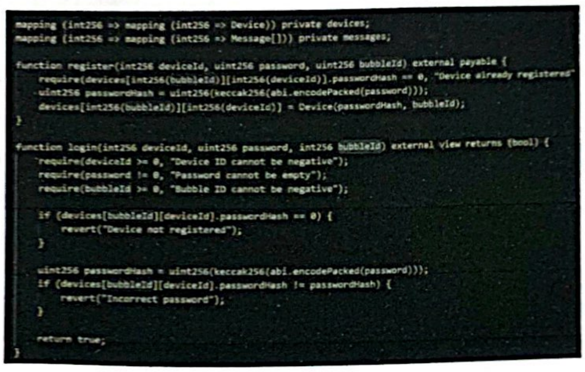
Figure 3.2.3 and 3.2.4 below shows the smart contracts programmed to implement the proposed model. This smart contracts function is to create bubble IDs and assign them. After assigning it does also verify it amongst the identifies devices within the same bubble they are in. This smart contract also has the function to send and receive messages between identified devices.



Smart Contract

```
struct Device {
          uint256
passwordHash;
          uint256 bubbleId;
     }

struct Message {
    int256 senderId;
    int256
receiverId;
    uint256
senderBubbleId;
    uint256
mapping (int256 => mapping (int256 => Device)) private devices;
mapping (int256 => mapping (int256 => Message[])) private
messages;
```

Figure 3.2.3: smart contract function of our system

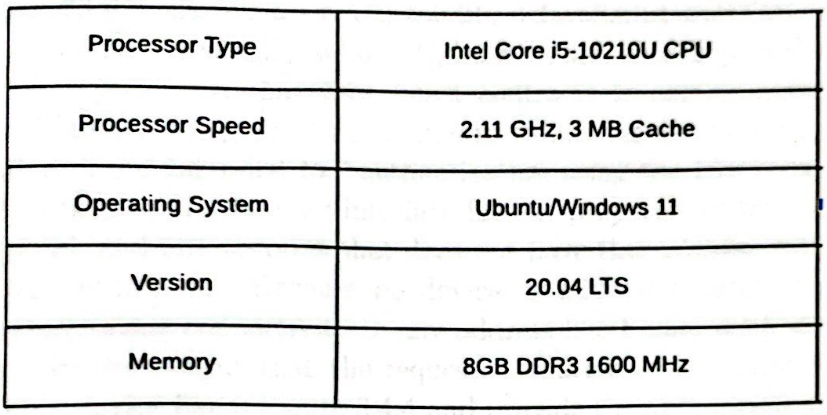


```
mapping (int256 => mapping (int256 => Device)) private devices;
mapping (int256 => mapping (int256 => Message[])) private messages;

function register(int256 deviceId, uint256 password, uint256 bubbleId) external payable {
    require(devices[int256(bubbleId)][int256(deviceId)].passwordHash == 0, "Device already registered"
    uint256 passwordHash = uint256(keccak256(abi.encodePacked(password)));
    devices[int256(bubbleId)][int256(deviceId)] = Device(passwordHash, bubbleId);
}

function login(int256 deviceId, uint256 password, int256 bubbleId) external view returns (bool) {
    require(deviceId >= 0, "Device ID cannot be negative");
    require(password != 0, "Password cannot be empty");
    require(bubbleId >= 0, "Bubble ID cannot be negative");

    if (devices[bubbleId][deviceId].passwordHash == 0) {
        revert("Device not registered");
    }

    uint256 passwordHash = uint256(keccak256(abi.encodePacked(password)));
    if (devices[bubbleId][deviceId].passwordHash != passwordHash) {
        revert("Incorrect password");
    }

    return true;
}
```

Figure 3.2.4: smart contract function of our system

3.3 Experimental Setup

For the implementation of our simulation, we employed a computer with a core i5, 10Th generation with CPU 1.60GHz 2.11GHz. The processor in question is equipped with two cores and four threads. Our CPU has an optimal clock speed of 2.3 GHz and 3 MB cache capacity. For implementation testing, we use Windows 11 as an operating system but Ubuntu 20.04 LTS can be used. In addition, our machine had 8 Gigabytes of RAM installed. Table figure? below illustrates the system configuration in which we will build the blockchain that we will use.

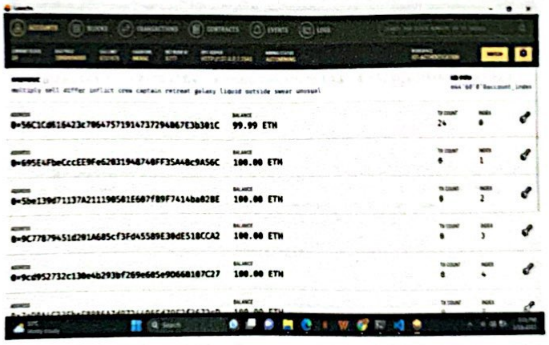


Processor Type	Intel Core i5-10210U CPU
Processor Speed	2.11 GHz, 3 MB Cache
Operating System	Ubuntu/Windows 11
Version	20.04 LTS
Memory	8GB DDR3 1600 MHz

Figure 3.3.1: Experimental Configuration

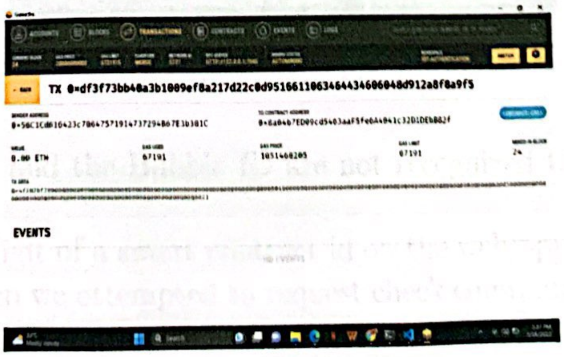
3.4 Implementation

We can set up a private blockchain on our personal devices by creating a Genesis block. Then we'll be able to build and deploy our very own private blockchain. We chose the Truffle framework Ganache for simplicity of processing to deploy our smart contract. Truffle's Ganache is a personal blockchain that allows users to easily install and develop dApps. Ganache is shown booting up on our machine in Figure 3.4.1. Ganache then gives us ten Ethereum accounts, each with 100 ethers and running on a private blockchain. Because our blockchain is based on Ganache, we must install a smart contract. For this, we used the visual studio code IDE and NODE JS. We wrote our solidity +JavaScript +(HTML, CSS) code for the front end on the visual studio IDE, built it, and then deployed it. We also created a web application that uses smart contracts to communicate with our blockchain. Figure 4.4 depicts the system's initialization. It is a straightforward representation of our intended IoT authentication using the Blockchain concept. Consider this page to be the user interface for our proposed system. Our device has a unique id, and any account that does not have that address will be denied access to our blockchain. Because no device or address is maintained on our blockchain, requesting connectivity to any address like Figure 3.4.6 after startup would result in the output that the requested address is not connected. If we try to set up a device like a Figure 3.4.4 and provide the appropriate inputs that include user device-id, password, and email for two-factor authentication purposes for the registration part.



```
multiply sell differ inflict crew captain retreat galaxy liquid outside swear unusual

0x56C1Cd616423c70647571914737294867E3b301C   99.99 ETH    24   0
0x695E4FbeCccEE9Fe62031948740FF35A48c9A56C   100.00 ETH   0    1
0x5be139d71137A211190501E607f89F7414ba028E   100.00 ETH   0    2
0x9C77879451d201A685cf3Fd45589E30dE518CCA2   100.00 ETH   0    3
0x9cd952732c130e4b293bf269e605e90668107C27   100.00 ETH   0    4
```

Figure 3.4.1: ganache interface



```
TX 0xdf3f73bb40a3b1009ef8a217d22c0d9516611063464434606048d912a8f8a9f5

SENDER ADDRESS                                 TO CONTRACT ADDRESS
0x56C1Cd616423c70647571914737294B67E3b301C     0x6a04b7ED09cd5403aaF5fe0A4941c32D1DEbB82f

VALUE       GAS USED    GAS PRICE     GAS LIMIT    MINED IN BLOCK
0.00 ETH    67191       1051460205    67191        24

EVENTS
```

Figure 3.4.2: transaction

User registration consists of the user device id and Bubble ID since already part of a bubble and an email where a unique ID will be assigned for login purposes or two Factor Authentication.

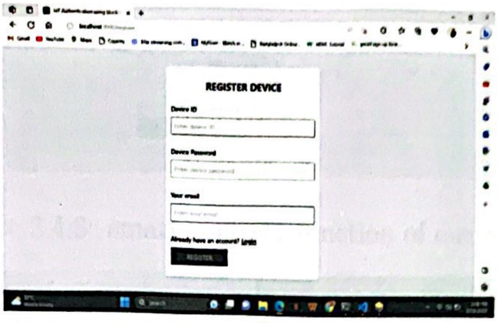
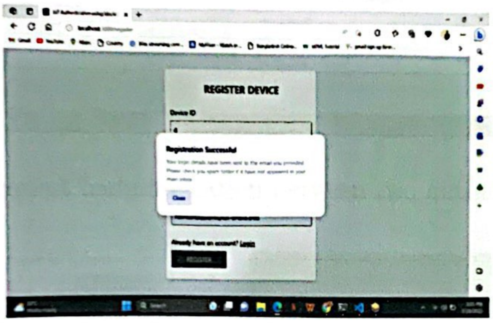


Figure 3.4.3: registration



Registration Successful

Your login details have been sent to the email you provided. Please check you spam folder if it have not appeared in your main inbox.

Figure 3.4.4: Successful Registration

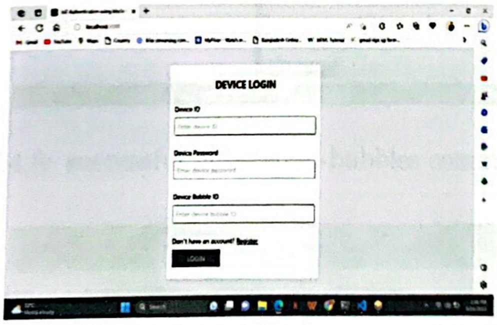
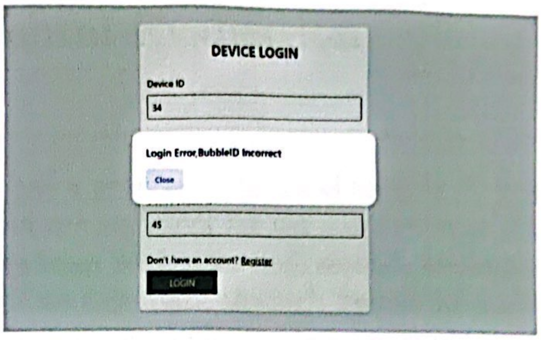


Figure 3.4.5: Login

if the device ID and the Bubble ID are not recognized then the user cannot log in

We modified a digit of a smart contract id on the web application for the purpose of testing. Then we attempted to request check communication and received the probable breach output displayed in Figure 3.4.8. This notification leaves us with the conclusion that if any digit in the system's configuration is incorrect, it will be identified and the instruction may be provided as needed.



DEVICE LOGIN

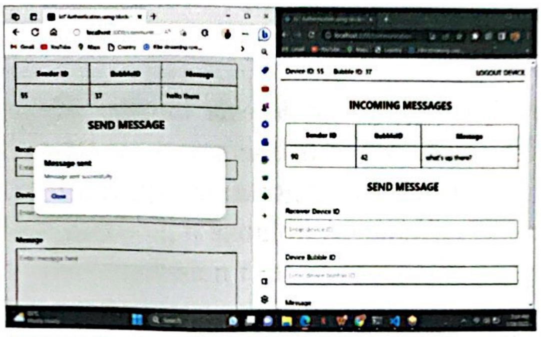
Device ID: 34

Login Error,BubbleID Incorrect

45

Don't have an account? Register

Figure 3.4.6: smart contract function of our system



Sender ID	BubbleID	Message
55	37	hello there

SEND MESSAGE

Message sent

Message sent successfully

Message: Enter message here

Device ID 55 Bubble ID 37

INCOMING MESSAGES

Sender ID	BubbleID	Message
90	42	what's up there?

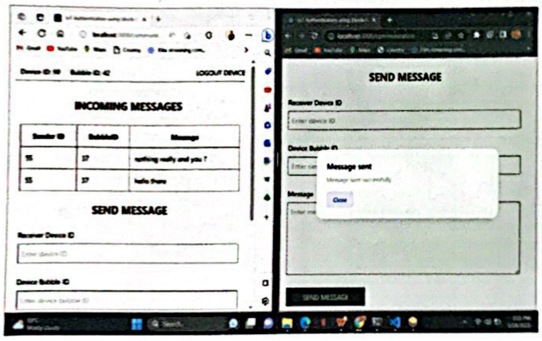
SEND MESSAGE

Receiver Device ID: Enter device ID

Device Bubble ID: Enter device bubble ID

Message

Figure 3.4.7: request communication between two authenticated devices



Device ID 90 Bubble ID 42

INCOMING MESSAGES

Sender ID	BubbleID	Message
55	37	nothing really and you ?
55	37	hello there

SEND MESSAGE

Receiver Device ID: Enter device ID

Device Bubble ID: Enter device bubble ID

SEND MESSAGE

Receiver Device ID: Enter device ID

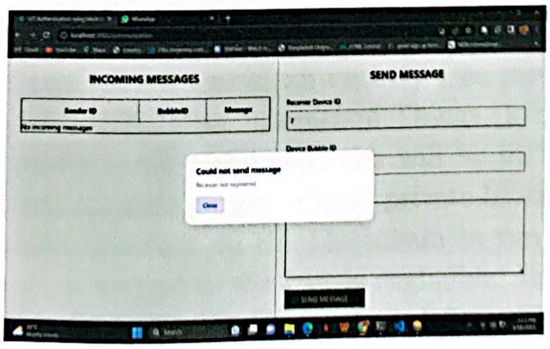
Device Bubble ID

Message sent

Message sent successfully

Message: Enter message here

Figure 3.4.8: successful in between-bubbles communication



INCOMING MESSAGES

Sender ID	BubbleID	Message
No incoming messages		

SEND MESSAGE

Receiver Device ID: 7

Device Bubble ID

Could not send message

Receiver not registered

Figure 3.4.9: device not recognized

4 Experimental Evaluation

4.1 Speed

Ethereum currently has a processing speed of roughly 30 transactions per second. Ten inputs per second are sufficient for our simulation in the proposed system. If we must register more than 20 devices each second, we simply have to consider the speed. Since we have to take data through human interaction, getting up to 20 inputs in a second is extremely difficult. As a result of this, our system is unlikely to encounter speed issues.

4.2 Storage

Graphic 4.2.1 depicts the current size of the Ethereum blockchain, which grows by the day as more blocks are being added to the chain. We only stored a list of Ethereum addresses as a string generating a lengthy block in our proposed design. Based on the look of our method, it shouldn't require an excessive amount of blocks of data, leading us to the conclusion that memory will be more than adequate.

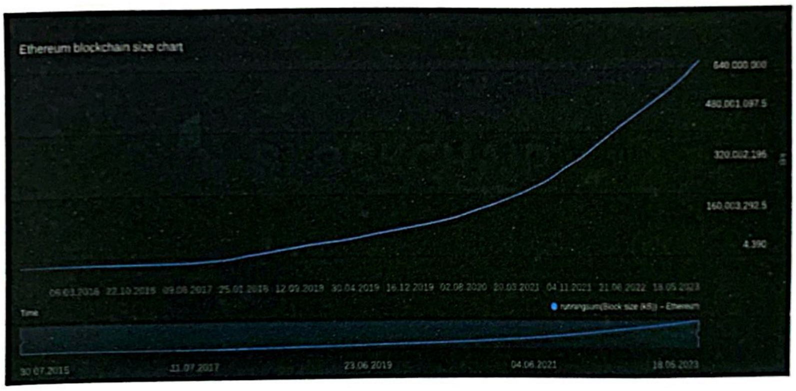
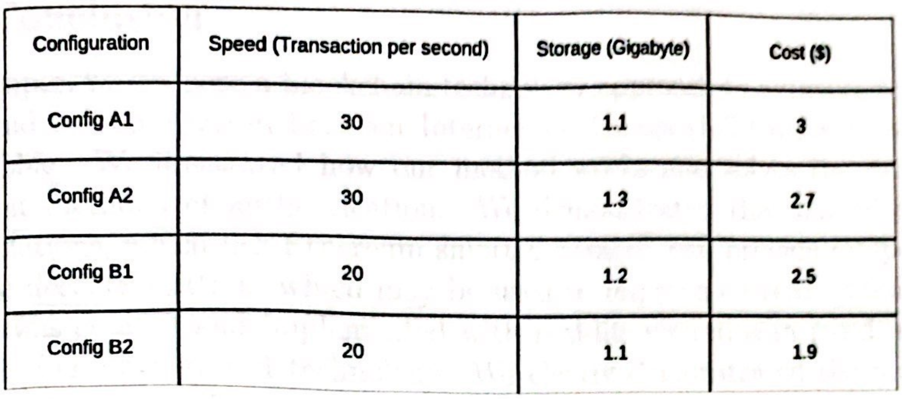


Figure 4.2.1: Ethereum current storage size

4.3 Cost

Our suggested approach makes use of an entirely free private local blockchain. If we are able to run blockchain on Internet of Things (IoT) devices in the near future, the cost of implementing this approach will be little. For it to function effectively, our proposal requires simply a local private blockchain operating 24/7 and our deployed smart contract on the blockchain to run correctly. Ethereum from a local blockchain is virtual so the cost is negligible. But if we are interested in implementing this approach in a huge number of devices or across an extensive area, such as a community, we may need to make modifications to the concept. Turning on a blockchain that is accessible to everyone will be beneficial.

4.4 Evaluation



Configuration	Speed (Transaction per second)	Storage (Gigabyte)	Cost ($)
Config A1	30	1.1	3
Config A2	30	1.3	2.7
Config B1	20	1.2	2.5
Config B2	20	1.1	1.9

Figure 4.4.1: Evaluation of the system

Here in the table config A1 and A2 represents the conventional or current method and config B1 and B2 represents the proposed or implemented method. These two method, which is both the current and proposed method have been tested and then compared in the three parameters which are speed, storage and cost.

5 Conclusion and Future Work

5.1 Conclusion

In this paper, we propose a blockchain technology approach to authenticate users' access and communication between Internet of Things (IoT) devices registered to a bubble. We illustrated how our method works and solves the drawbacks of present methods of authentication. We demonstrated that our blockchain-based solutions, which use Ethereum smart contracts, can provide tamper-proof data and decentralization, which may be used to improve current systems. Our solution was created and implemented with real-life scenarios in mind, utilizing accessible IoT devices and technology. We clearly demonstrated the process of authenticating users who are authorized in order for them to communicate safely using IoT devices. We also demonstrated that our technique was able to deal with designed assaults attempting to attack legitimate connections and forcefully obtain credentials. Despite the encouraging results, there are still significant obstacles to overcome, including scalability and interoperability.

5.2 Future work

We are planning to expand on this thesis work in the future in a way that our proposed solution is capable to be used for large-scale connectivity and authentication to a huge number of bubbles with IoT devices and end users. We are also looking forward to research more to find more secured mechanism and easier ways to authenticate the devices in IoT.

References

[1] @articlehammi2018bubbles, title=Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, author=Hammi, Mohamed Tahar and Hammi, Badis and Bellot, Patrick and Serhrouchni, Ahmed, journal=Computers and Security, volume=78, pages=126–142, year=2018, publisher=Elsevier

[2] @inproceedingsalphand2018iotchain, title=IoTChain: A blockchain security architecture for the Internet of Things, author=Alphand, Olivier and Amoretti, Michele and Claeys, Timothy and Dall'Asta, Simone and Duda, Andrzej and Ferrari, Gianluigi and Rousseau, Franck and Tourancheau, Bernard and Veltri, Luca and Zanichelli, Francesco, booktitle=2018 IEEE wireless communications and networking conference (WCNC), pages=1–6, year=2018, organization=IEEE

[3] @articlemohanta2020addressing, title=Addressing security and privacy issues of IoT using blockchain technology, author=Mohanta, Bhabendu Kumar and Jena, Debasish and Ramasubbareddy, Somula and Daneshmand, Mahmoud and Gandomi, Amir H, journal=IEEE Internet of Things Journal, volume=8, number=2, pages=881–888, year=2020, publisher=IEEE

[4] @articlebagga2022blockchain, title=Blockchain-envisioned access control for internet of things applications: A comprehensive survey and future directions, author=Bagga, Palak and Das, Ashok Kumar and Chamola, Vinay and Guizani, Mohsen, journal=Telecommunication Systems, volume=81, number=1, pages=125–173, year=2022, publisher=Springer

[5] @articleali2020xdbauth, title=xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things, author=Ali, Gauhar and Ahmad, Naveed and Cao, Yue and Khan, Shahzad and Cruickshank, Haitham and Qazi, Ejaz Ali and Ali, Azaz, journal=IEEE Access, volume=8, pages=58800–58816, year=2020, publisher=IEEE

[6] @inproceedingsbanoun2021iot, title=IoT-BDMS: securing IoT devices with hyperledger fabric blockchain, author=BANOUN, Nathalie and DIARRA, Nafissatou and others, booktitle=CS & IT Conference Proceedings, volume=11, number=6, year=2021, organization=CS & IT Conference Proceedings

[7] @inproceedingsourad2018using, title=Using blockchain for IOT access control and authentication management, author=Ourad, Abdallah Zoubir and Belgacem, Boutheyna and Salah, Khaled, booktitle=Internet of Things–ICIOT 2018: Third International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25-30, 2018, Proceedings 3, pages=150–164, year=2018, organization=Springer

[8] @inproceedingsrashid2019security, title=A security framework for IoT authentication and authorization based on blockchain technology, author=Rashid, Mohammed A and Pajooh, Houshyar Honar, booktitle=2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pages=264–271, year=2019, organization=IEEE

[9] @inproceedingsshakarami2022blockchain, title=Blockchain-based administration of access in smart home iot, author=Shakarami, Mehrnoosh and Benson, James and Sandhu, Ravi, booktitle=Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, pages=57–66, year=2022

[10] @articlevairagade2020study, title=A study of various authentication mechanisms towards the secure Internet of Things networks, author=Vairagade, Rupali Sachin and Brahmananda, SH, journal=Control and Cybernetics, volume=49, number=4, pages=393–418, year=2020, publisher=Polska Akademia Nauk. Instytut Badań Systemowych PAN

[11] @articleferreira2021iot, title=IoT registration and authentication in smart city applications with blockchain, author=Ferreira, Célio Márcio Soares and Garrocho, Charles Tim Batista and Oliveira, Ricardo Augusto Rabelo and Silva, Jorge Sá and Cavalcanti, Carlos Frederico Marcelo da Cunha, journal=Sensors, volume=21, number=4, pages=1323, year=2021, publisher=MDPI

[12] @articlesehar2023blockchain, title=Blockchain enabled data security in vehicular networks, author=Sehar, Naseem us and Khalid, Osman and Khan, Imran Ali and Rehman, Faisal and Fayyaz, Muhammad AB and Ansari, Ali R and Nawaz, Raheel, journal=Scientific Reports, volume=13, number=1, pages=4412, year=2023, publisher=Nature Publishing Group UK London

[13] @articlehameed2021formally,

title=A formally verified blockchain-based decentralised authentication scheme for the internet of things, author=Hameed, Khizar and Garg, Saurabh and Amin, Muhammad Bilal and Kang, Byeong, journal=The Journal of Supercomputing, volume=77, number=12, pages=14461–14501, year=2021, publisher=Springer

[14] @articlegong2021bcot, title=BCoT sentry: A blockchain-based identity authentication framework for IoT devices, author=Gong, Liangqin and Alghazzawi, Daniyal M and Cheng, Li, journal=Information, volume=12, number=5, pages=203, year=2021, publisher=MDPI

[15] @articleal2023authentication, title=Authentication-Chains: Blockchain-Inspired Lightweight Authentication Protocol for IoT Networks, author=Al Ahmed, Mahmoud Tayseer and Hashim, Fazirulhisyam and Hashim, Shaiful

Jahari and Abdullah, Azizol, journal=Electronics, volume=12, number=4, pages=867, year=2023, publisher=MDPI

[16] @inproceedingsvalentin2021blockchain, title=A Blockchain-based Access and Management System for IoT Devices, author=Valentin, Manuel and Pahl, Claus and El Ioini, Nabil and Barzegar, Hamid R, booktitle=2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pages=1–8, year=2021, organization=IEEE

[17] @articleferrag2020security, title=Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges, author=Ferrag, Mohamed Amine and Shu, Lei and Yang, Xing and Derhab, Abdelouahid and Maglaras, Leandros, journal=IEEE access, volume=8, pages=32031–32053, year=2020, publisher=IEEE

[18] @articlesarmah2018understanding, title=Understanding blockchain technology, author=Sarmah, Simanta Shekhar, journal=Computer Science and Engineering, volume=8, number=2, pages=23–29, year=2018

[19] @inproceedingssu2018smartsupply, title=SmartSupply: Smart contract based validation for supply chain blockchain, author=Su, Shuang and Wang, Ke and Kim, Hyong S, booktitle=2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), pages=988–993, year=2018, organization=IEEE

[20] @articlechytisreview, title=A Review of Blockchain Technology and Its Applications in the Business Environment, author=Chytis, Evangelos

[21] @articlesyed2022zero, title=Zero trust architecture (zta): A comprehensive survey, author=Syed, Naeem Firdous and Shah, Syed W and Shaghaghi, Arash and Anwar, Adnan and Baig, Zubair and Doss, Robin, journal=IEEE Access, year=2022, publisher=IEEE

[22] @articlehao2018collaborative, title=A collaborative PHY-aided technique for end-to-end IoT device authentication, author=Hao, Peng and Wang, Xianbin and Shen, Weiming, journal=IEEE Access, volume=6, pages=42279–42293, year=2018, publisher=IEEE

[23] @articlekamboj2021user, title=User authentication using Blockchain based smart contract in role-based access control, author=Kamboj, Priyanka and Khare, Shivang and Pal, Sujata, journal=Peer-to-Peer Networking and Applications, volume=14, number=5, pages=2961–2976, year=2021, publisher=Springer

[24] @articlejoshi2021unified, title=Unified authentication and access control for future mobile communication-based lightweight IoT systems using blockchain, author=Joshi, Shubham and Stalin, Shalini and Shukla, Prashant Kumar

and Shukla, Piyush Kumar and Bhatt, Ruby and Bhadoria, Rajan Singh and Tiwari, Basant, journal=Wireless Communications and Mobile Computing, volume=2021, pages=1–12, year=2021, publisher=Hindawi Limited

[25] @inproceedingsli2019touch, title=Touch well before use: Intuitive and secure authentication for iot devices, author=Li, Xiaopeng and Yan, Fengyao and Zuo, Fei and Zeng, Qiang and Luo, Lannan, booktitle=The 25th annual international conference on mobile computing and networking, pages=1–17, year=2019

[26] @inproceedingsshah2020towards, title=Towards a lightweight continuous authentication protocol for device-to-device communication, author=Shah, Syed Wajid Ali and Syed, Naeem Firdous and Shaghaghi, Arash and Anwar, Adnan and Baig, Zubair and Doss, Robin, booktitle=2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pages=1119–1126, year=2020, organization=IEEE

[27] @articlemohanta2020addressing, title=Addressing security and privacy issues of IoT using blockchain technology, author=Mohanta, Bhabendu Kumar and Jena, Debasish and Ramasubbareddy, Somula and Daneshmand, Mahmoud and Gandomi, Amir H, journal=IEEE Internet of Things Journal, volume=8, number=2, pages=881–888, year=2020, publisher=IEEE

[28] @articleal2022cab, title=CAB-IoT: Continuous authentication architecture based on Blockchain for internet of things, author=Al-Naji, Fatimah Hussain and Zagrouba, Rachid, journal=Journal of King Saud University-Computer and Information Sciences, volume=34, number=6, pages=2497–2514, year=2022, publisher=Elsevier

[29] @articlekhalid2020decentralized, title=A decentralized lightweight blockchain-based authentication mechanism for IoT systems, author=Khalid, Umair and Asim, Muhammad and Baker, Thar and Hung, Patrick CK and Tariq, Muhammad Adnan and Rafferty, Laura, journal=Cluster Computing, volume=23, number=3, pages=2067–2087, year=2020, publisher=Springer