

DAYANANDA SAGAR UNIVERSITY

### KUDLU GATE, BANGALORE - 560068

**Bachelor of Technology in**

**COMPUTER SCIENCE AND ENGINEERING**

**Major Project Phase - II Report**

**(Blockchain Based Authentication For IOT Devices)**

By

**SANDHYA M- ENG20CS0317**

**SHAREEBA N- ENG20CS0332**

**SOWMYA M K- ENG20CS0356**

**SURAVI R - ENG20CS0373**

**Under the supervision of**

#### Prof. VEDASHREE L V

#### Assistant Professor, Dept of CS&E

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,**

### SCHOOL OF ENGINEERING DAYANANDA SAGAR UNIVERSITY,

**(2023-2024)**



DAYANANDA SAGAR UNIVERSITY

**KUDLU GATE, BANGALORE – 560068**

**Department of Computer Science & Engineering**

# CERTIFICATE

This is to certify that the Major Project Stage-I work titled **“BLOCKCHAIN BASED AUTHENTICATION SYSTEM FOR INTERNET OF THINGS”** is carried out by Sandhya M (ENG20CS0317), Shareeba N (ENG20CS0332), Sowmya M K(ENG20CS0356), Suravi R(ENG20CS0373), bonafide students of Bachelor of Technology in Computer Science and Engineering at the School of Engineering, Dayananda Sagar University, Bangalore in partial fulfillment for the award of degree in Bachelor of Technology in Computer Science and Engineering, during the year 2023-2024.

|  |  |  |
| --- | --- | --- |
| **Prof Vedashree L V** | **Dr. Girisha G S** | **Dr. Udaya Kumar Reddy K R** |
| Assistant Professor Dept. of CS&E, School of Engineering  Dayananda Sagar University | Chairman CSE School of Engineering  Dayananda Sagar University | Dean  School of Engineering Dayananda Sagar University |
| Date: | Date: | Date: |

##### Name of the Examiner Signature of

**Examiner**

1.

2.

# DECLARATION

We, **Sandhya M (ENG20CS0317), Shareeba N (ENG20CS0332), Sowmya M K (ENG20CS0356), Suravi R (ENG20CS0373),** are students of 8th semester B. Tech in **Computer Science and Engineering**, at School of Engineering, **Dayananda Sagar University**, hereby declare that the Major Project Stage-I titled **“ BLOCKCHAIN BASED AUTHENTICATION SYSTEM FOR ITERNET OF THINGS”** has been carried out by us and submitted in partial fulfillment for the award of degree in **Bachelor of Technology in Computer Science and Engineering** during the academic year **2023-2024.**

**Student Signature**

**Name : Sandhya USN : ENG20CS0317**

**Name : Shareeba N**

**USN : ENG20CS0332**

**Name : Sowmya M K USN : ENG20CS0356**

**Name : Suravi R**

**USN : ENG20CS0373**

**Place : Bangalore Date :**

## ACKNOWLEDGEMENT

*It is a great pleasure for us to acknowledge the assistance and support of many individuals who have been responsible for successful completion of this project work.*

*First, we take this opportunity to express our sincere gratitude to the School of Engineering & Technology, Dayananda Sagar University for providing us with a great opportunity to pursue our Bachelor’s degree in this institution.*

*We would like to thank* ***Dr. Udaya Kumar Reddy K R, Dean, School of Engineering & Technology, Dayananda Sagar University*** *for his constant encouragement and expert advice.*

*It is a matter of immense pleasure to express our sincere thanks to* ***Dr. Girisha G S, Chairman, Computer Science and Engineering, Dayananda Sagar University,*** *for providing the right academic guidance that made our task possible.*

*We would like to thank our guide* ***Prof Vedashree L V, Assistant Professor, Dept. of Computer Science and Engineering, Dayananda Sagar University,*** *for sparing his valuable time to extend help in every step of our project work, which paved the way for smooth progress and fruitful culmination of the project.*

*We would like to thank our* ***Project Coordinator Dr. Meenakshi Malhotra*** *and* ***Prof. Mohammed Khurram J*** *as well as all the staff members of Computer Science and Engineering for their support.*

*We are also grateful to our family and friends who provided us with every requirement throughout the course.*

*We would like to thank one and all who directly or indirectly helped us in the Project*

*work.*

## TABLE OF CONTENTS

**Title Page. No**

[LIST OF ABBREVIATIONS](#page7)…………………………………………………………….. v

[LIST OF FIGURES](#page8)………………………………………………………………………. vi

[ABSTRACT](#page8)……………………………………………………………………………… vii

CHAPTER 1 INTRODUCTION………............................................................................... 1

1.1. SCOPE…………………………………………………………………………... 1

CHAPTER 2 PROBLEM DEFINITION ……….................................................................. 2

CHAPTER 3 LITERATURE SURVEY…………………………………………………… 3

CHAPTER 4 PROJECT DESCRIPTION 6

4.1. PROPOSED DESIGN…………………………………………………………... 6

CHAPTER 5 REQUIREMENTS………………………………………………………….. 8

5.1. FUNCTIONAL REQUIREMENTS…………………………………………….. 8

5.2. NON-FUNCTIONAL REQUIREMENTS……………………………………… 9

5.3. SOFTWARE REQUIREMENTS……………………………………………….. 9

5.4. HARDWARE REQUIREMENTS……………………………………………… 10

CHAPTER 6 METHODOLOGY…………………………………………………………... 11

CHAPTER 7 EXPERIMENTATION……………………………………………………... 12

CHAPTER 8 RESULTS…………………………………………………………………… 13

CONCLUSION……………………………………………………………………………… 15

REFERENCES .................................................................................................................... 16

Appendix – 1 …………………………………………………………………………………17

# ABBREVIATIONS USED

|  |  |
| --- | --- |
| IOT | Internet Of Things |
|  |  |
| ECC | Elliptic Curve Cryptography |
|  |  |
| MATLAB | Matrix laboratory |
|  |  |
|  |  |
| GUI | Graphical User Interfaces |
|  |  |

## LIST OF FIGURES

|  |  |  |
| --- | --- | --- |
| Fig. No. | Description of the figure | Page No. |
|  |  |  |
| 4.1(a) | Registration | 6 |
|  |  |  |
| 4.1(b) | Authentication | 7 |
|  |  |  |
| 7.1(a) | UI Design | 13 |
|  |  |  |
| 7.1(b) | App Design | 13 |
|  |  |  |
| 7.1(c) | Authenticated Communication | 14 |
|  |  |  |

# Abstract

The rapid expansion of the Internet of Things (IoT) introduces complex security challenges, particularly in the areas of device authentication, data integrity, and decentralized management. Traditional security mechanisms often fall short in addressing these issues due to the unique constraints and scalability requirements of IoT networks. In response, this project proposes a secure, blockchain-based framework for IoT device registration and authentication, implemented in MATLAB. Utilizing the principles of Elliptic Curve Cryptography (ECC) for cryptographic key generation, our framework ensures a high level of security that is both efficient and scalable, suitable for the diverse ecosystem of IoT devices. Through the integration of blockchain technology, we offer a decentralized approach to IoT security, enhancing data integrity and device authenticity across the network. The proposed MATLAB simulation provides a practical and accessible platform for exploring the application of blockchain in securing IoT devices, demonstrating the framework's effectiveness in real-world scenarios. This work not only addresses the immediate security concerns of IoT networks but also lays the groundwork for future research and development in the convergence of blockchain technology and IoT security solutions.

# CHAPTER 1 INTRODUCTION

**CHAPTER 1 INTRODUCTION**

The Internet of Things (IoT) has emerged as a transformative force in the digital age, heralding a new era where everyday objects are interconnected and communicate over the internet. This proliferation of IoT devices offers unparalleled opportunities for innovation across various sectors, including healthcare, agriculture, smart cities, and industrial automation. However, the rapid expansion and integration of these devices into critical infrastructures have also exposed significant security vulnerabilities. Among these, ensuring the authenticity and integrity of devices and their data remains a paramount challenge. Traditional security mechanisms often struggle to cope with the sheer scale and diversity of IoT environments, leading to an urgent need for novel solutions that can ensure robust security without compromising on scalability or device performance. Blockchain technology, best known for underpinning cryptocurrencies like Bitcoin, has been identified as a promising solution to these challenges. Its decentralized nature, combined with strong cryptographic foundations, offers a new paradigm for secure, transparent, and tamper proof systems. In the context of IoT, blockchain can facilitate secure device registration, authentication, and data exchange, creating a thrustless environment where devices can operate securely and autonomously.

**1.1. SCOPE**

This project introduces a novel framework for the registration and authentication of IoT devices using a blockchain-based approach, implemented within the MATLAB environment. By leveraging Elliptic Curve Cryptography (ECC), our framework offers a balance between security and efficiency, making it well-suited for the diverse and resource-constrained IoT ecosystem. We discuss the design and implementation of this framework, focusing on its potential to enhance IoT security through a decentralized, transparent, and tamper-proof system. Our work aims to bridge the gap between the theoretical potential of blockchain technology and its practical application in securing IoT devices, providing a foundation for further research and development in this critical area.

# CHAPTER 2 PROBLEM DEFINITION

**CHAPTER 2 PROBLEM DEFINITION**

**PROBLEM STATEMENT**

The integration of Internet of Things (IoT) devices into interconnected networks poses significant security challenges, particularly regarding authentication. Traditional centralized authentication systems struggle to accommodate the dynamic and heterogeneous nature of IoT environments, leading to potential vulnerabilities and single points of failure. Additionally, the resource-constrained nature of many IoT devices further complicates the implementation of robust security measures. Thus, there is an urgent need for decentralized and resilient authentication mechanisms tailored specifically for IoT devices to ensure secure interactions within IoT ecosystems.

**SOLUTION**

In response to the aforementioned challenges, this project proposes the development and implementation of blockchain-based authentication mechanisms within the MATLAB environment. Leveraging the decentralized and immutable nature of blockchain technology, the proposed solution aims to provide a secure and scalable authentication framework for IoT devices. By employing Elliptic Curve Cryptography (ECC) for key pair generation and blockchain protocols for transaction verification and consensus, the solution seeks to enhance the security and integrity of IoT networks. Furthermore, the solution endeavors to address the resource constraints of IoT devices by optimizing blockchain protocols for efficiency and lightweight operation. Through practical demonstrations and empirical evaluations, the proposed solution aims to validate its efficacy in fortifying authentication processes for IoT devices within MATLAB-based IoT deployments.

# CHAPTER 3 LITERATURE REVIEW

**CHAPTER 3 LITERATURE REVIEW**

The literature surrounding blockchain-based authentication for IoT devices encompasses a diverse range of studies, exploring various aspects of security, scalability, and practical implementation. Several key themes emerge from the existing body of research, providing valuable insights into the challenges and opportunities in this domain.

[1], this paper introduces a comprehensive approach to blockchain-based authentication within IoT networks. By leveraging blockchain technology, this system revolutionizes the conventional methods by eliminating the necessity for a centralized authority, thus significantly enhancing security and privacy. Its impact is underscored by its citation in 25 other papers, highlighting its relevance and influence in the field of IoT security.

1. presents a groundbreaking authentication mechanism tailored specifically for fog computing environments. With a keen eye on performance improvement, this mechanism demonstrates remarkable advancements compared to existing methods. Its contribution is particularly significant as fog computing gains momentum in IoT ecosystems, demanding robust and efficient authentication protocols.

[3], This is a novel decentralized authentication framework for IoT networks proposed , harnessing the power of blockchain technology. This approach not only fortifies security but also enhances privacy by decentralizing authentication processes. By eliminating reliance on a centralized authority, it addresses a critical vulnerability in traditional authentication mechanisms.

[4] The authentication protocol outlined in this paper introduces a paradigm shift in IoT access control, emphasizing capability-based authorization facilitated by blockchain. This innovative approach promises to mitigate security risks while ensuring scalability, thus laying the groundwork for robust and flexible IoT ecosystems.

.

[5]Presents a pioneering hypergraph-based blockchain model tailored for smart homes in IoT environments. This model, combining hypergraph representation and blockchain technology, offers a decentralized and immutable record of device interactions, bolstering security and privacy in smart home settings.

[6] The lightweight consensus algorithm proposed is also known as Proof-of-Authentication (PoAh), is a game changer for resource-constrained IoT edge nodes. By leveraging blockchain principles, PoAh tackles scalability and security challenges inherent in IoT networks, paving the way for efficient and resilient IoT ecosystems.

[7] The exploration of sidechains within blockchain-enabled IoT systems introduces a novel consensus protocol, promising enhanced functionality and security. Sidechains offer scalability and customization, augmenting traditional blockchains with new functionalities and privacy features, thus enriching the IoT landscape.

1. This paper showcases a transformative block chain-based IoT application utilizing smart contracts for M2M autonomous trading. This application demonstrates the tangible benefits of blockchain and smart contracts in managing IoT devices and transactions securely and efficiently. The presented case study underscores the viability of blockchain technology in real-world IoT applications.

[9],In this paper, a decentralized block chain-based key management (KM) protocol tailored for resource-constrained IoT devices is proposed. This protocol strategically balances node loads based on their capabilities, offering scalability, security, and efficiency within a distributed IoT architecture. Simulations and experiments validate its effectiveness, reflecting its relevance in block chain-based IoT architectures, data management, and access control.

1. introduces a blockchain-based dynamic access control scheme finely crafted for IoT networks. Leveraging smart contracts, this scheme orchestrates access control policies with a consensus algorithm, ensuring both security and efficiency. Its versatility makes it applicable across various IoT scenarios, earning recognition in studies on blockchain-based IoT access control and dynamic access control systems.

[11] The Block chain-based Trust Management Scheme for IoT outlined in this paper pioneers a robust solution for enhancing trust relationships and fortifying system security in IoT environments. By harnessing blockchain technology, this scheme offers a secure and efficient trust management framework tailored for IoT networks, addressing critical trust-related challenges.

1. contributes a blockchain-based authentication and access control framework meticulously designed for IoT networks. This scheme, underpinned by smart contracts and a consensus algorithm, provides a decentralized and tamper-proof solution to security challenges. Its versatility renders it applicable across various IoT scenarios, recognized in studies on IoT security, access control, and authentication.

[13] The framework presented lays the groundwork for a blockchain-based authentication and authorization framework specifically engineered for IoT networks. Utilizing smart contracts and a consensus algorithm, this framework elevates traditional access control methods, offering enhanced security and efficiency.

1. proposes a blockchain-based secure data-sharing scheme meticulously crafted for IoT environments. By employing end-to-end encryption and fine-grained access control mechanisms, this scheme addresses security and privacy concerns inherent in IoT data sharing. Its robustness and efficiency make it a cornerstone in studies focusing on IoT security, data sharing, and access control.

[15] This paper proposes a blockchain-based secure and decentralized resource management scheme for IoT networks is introduced. This scheme, powered by a consortium blockchain and smart contracts, revolutionizes resource allocation and access control in IoT ecosystems. Its deployment promises improved performance and reliability across various IoT applications, earning recognition in studies focusing on blockchain-based resource management and access control.

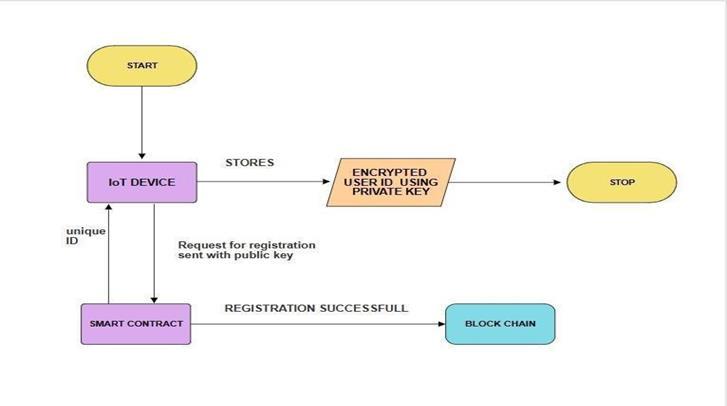
# CHAPTER 4 PROJECT DESCRIPTION

**CHAPTER 4 PROJECT DESCRIPTION**

**4.1. PROPOSED DESIGN**

The proposed design of our framework integrates blockchain technology with Elliptic Curve Cryptography (ECC) to address the security needs of IoT devices in a decentralized network. The design focuses on two main components: secure device registration and authentication, facilitated through a blockchain infrastructure.

**A. Secure Device Registration**



***Figure 4.1.(a) Registration***

The secure device registration process involves the following steps:

**Device Identity Generation:**

Each IoT device generates a unique cryptographic key pair using ECC. The private key remains securely stored on the device, while the corresponding public key is published on the blockchain.

**Blockchain Registration:**

The device public key, along with additional metadata such as device ID and attributes, is recorded on the blockchain as part of the device registration process. This creates a tamper-proof record of device identities on the decentralized ledger.

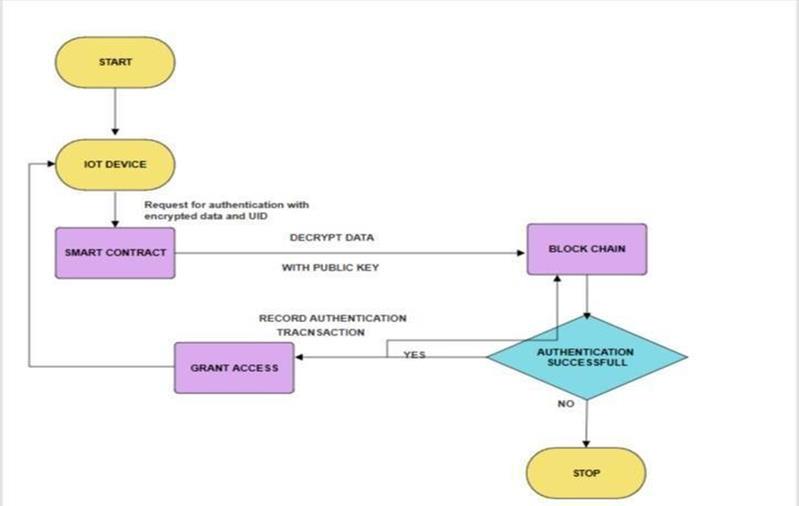
**Verification and Consensus:**

The registration transaction undergoes verification by network nodes through a consensus mechanism, ensuring the integrity and validity of the transaction before it is added to the blockchain.

**Immutable Ledger:**

Once registered, device identities are immutable and transparent, providing a trusted source of truth for device authentication and communication within the network.

**B. Authentication Process**



***Figure 4.1.(b) Authentication***

The authentication process builds upon the registered device identities stored on the blockchain:

**Signature Generation:**

When a device attempts to communicate within the network, it signs its messages using its private key.

This cryptographic signature serves as proof of the message's authenticity and origin.

**Public Key Retrieval:**

The receiving device or service retrieves the sender's public key from the blockchain, using it to verify the signature and authenticate the sender's identity.

**Verification and Trust Establishment:**

By validating the signature against the sender's public key, the receiving device can establish trust in the authenticity of the message and the identity of the sender, enabling secure communication and interaction between devices.

**Immutable Authentication Record:**

Authentication transactions are recorded on the blockchain, creating an immutable record of device interactions and ensuring traceability and accountability within the network.

# CHAPTER 5 REQUIREMENTS

**CHAPTER 5 REQUIREMENTS**

**5.1 FUNCTIONAL REQUIREMENTS**

* Registration Functionality: The system should allow IoT devices to initiate registration requests to establish their identity on the blockchain network.
* Smart contracts on the blockchain should validate registration requests and store device identifiers securely.
* Authentication Functionality: IoT devices should be able to initiate authentication requests to access network resources securely.
* The blockchain network should validate authentication requests and enforce access control based on predefined rules stored in smart contracts.
* Key Pair Generation: The system should generate cryptographic key pairs (public-private key pairs or ECC key pairs) for device registration and authentication.
* Key pair generation methods should ensure randomness and security to prevent unauthorized access.
* Blockchain Operations: The system should support blockchain operations such as adding blocks, validating blocks, and maintaining the integrity of the blockchain.
* Smart contracts should facilitate the execution of registration and authentication processes securely.

**5.2 NON-FUNCTIONAL REQUIREMENTS**

* Security: The system should prioritize security by employing cryptographic techniques to protect sensitive data and prevent unauthorized access.
* Measures should be in place to safeguard against common security threats such as replay attacks and data tampering.
* Performance: The system should demonstrate efficient performance in handling registration and authentication requests from multiple IoT devices simultaneously.
* Blockchain operations should be optimized for speed and scalability to accommodate the growing number of devices in the network.
* Reliability: The system should be reliable and resilient to failures, ensuring continuous operation even in the event of network disruptions or node failures.
  + Redundancy mechanisms should be in place to maintain the availability of critical services.

**5.3 SOFTWARE REQUIREMENTS:**

* MATLAB Environment: The system requires MATLAB software for running the blockchain based authentication application.
* MATLAB libraries or toolboxes may be utilized for cryptographic operations, blockchain implementation, and network communication.
* Blockchain Framework: The system may rely on existing blockchain frameworks or libraries compatible with MATLAB for blockchain operations.
* Smart contract development tools may be used for creating and deploying contract logic on the blockchain network

**5.4 HARDWARE REQUIREMENTS:**

* Computing Resources: The system requires sufficient computing resources to run MATLAB applications and support blockchain operations.
* Hardware specifications should meet the minimum requirements for running MATLAB efficiently.
* Networking Infrastructure: IoT devices should have access to reliable network connectivity to communicate with the blockchain network.
* Network infrastructure should support secure communication protocols to ensure data confidentiality and integrity

# CHAPTER 6 METHODOLOGY

**CHAPTER 6 METHODOLOGY**

Our methodology for implementing the proposed design in MATLAB involves several key steps:

* Simulation Environment Setup: The MATLAB environment is prepared with necessary libraries

and toolboxes for blockchain and ECC operations. This includes setting up functions for

cryptographic operations, blockchain ledger management, and network simulation.

* Key Generation and Registration: We simulate the process of key generation using ECC, ensuring

each IoT device is assigned a secure and unique cryptographic key pair. The public keys are then recorded on the blockchain as part of the device registration process, leveraging MATLAB's data-handling capabilities to manage the blockchain ledger.

* Blockchain Network Simulation: A simulated blockchain network is established within

MATLAB, allowing for the creation, validation, and addition of blocks to the ledger. This includes simulating the consensus mechanism to ensure the network's integrity and security.

* Device Authentication Process: The framework simulates the authentication process, where

devices validate each other's identities through cryptographic signatures before engaging in secure communications. This process leverages the public key infrastructure established on the blockchain, with MATLAB performing the cryptographic verifications.

* Performance and Security Analysis: Finally, the framework's performance and security are

analysed through MATLAB's analytical tools. This includes evaluating the efficiency of cryptographic operations, the scalability of the blockchain network, and the overall security of the device registration and authentication processes.

* Through this methodology, the proposed framework aims to demonstrate a practical and

scalable approach to enhancing IoT security using blockchain and ECC within a MATLAB simulation environment, providing a foundation for further research and development in this critical area.

# CHAPTER 7 EXPERIMENTATION

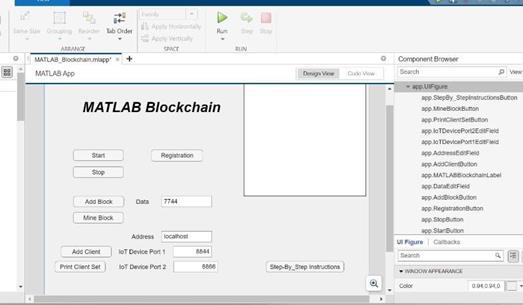
**CHAPTER 7 EXPERIMENTATION**

In this study, we detail an experimental setup leveraging MATLAB to simulate a rudimentary blockchain network, aimed at elucidating the core principles of node communication and data synchronization within distributed ledger technologies. The experiment commenced with the initialization of two independent MATLAB instances, each representing a node within the blockchain network. These instances were directed to a specifically designed demo application, runapp.m, which facilitated the graphical user interface for blockchain simulation. An integral part of the experiment involved intentionally misconfiguring the network settings to simulate a typical node communication error, thereby demonstrating the system's robustness and error handling capabilities. Subsequently, the network settings were corrected—by swapping the remote and local port numbers in one of the instances—to establish a successful communication link between the two nodes. The process of data addition and the subsequent mining of a new block on one node, followed by the replication of the newly mined block on the second node, effectively demonstrated the decentralized and distributed nature of blockchain networks. This experimental setup not only showcased the blockchain's ability to maintain data integrity and consistency across distributed nodes but also highlighted the practical challenges and considerations in configuring and managing a blockchain network. Through this study, we contribute to the ongoing discourse on blockchain technology, offering insights into its operational mechanisms and potential applications.

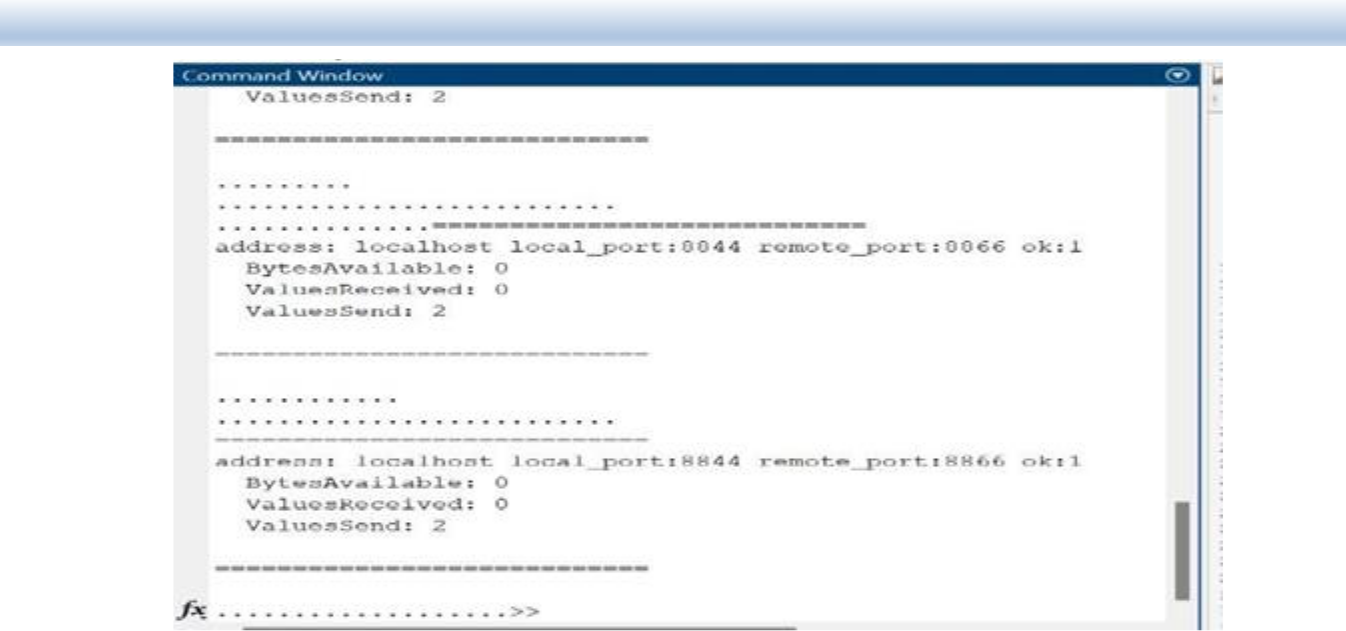
# CHAPTER 8 RESULTS

**CHAPTER 8 RESULTS**

***Figure 7.1.(a) UI Design***

****

***Figure 7.1.(b) App Design***



***Figure 7.1.(c)Authenticated Communication***

Overall, the experimentation results validate the effectiveness and robustness of the proposed framework for secure IoT device registration and authentication. Through MATLAB based simulations, we have demonstrated the framework's ability to efficiently manage device identities, authenticate devices securely, and maintain the integrity of the blockchain network.

# CHAPTER 9 CONCLUSION

**CHAPTER 9 CONCLUSION**

This project presented a blockchain-based framework for the secure registration and authentication of IoT devices, leveraging Elliptic Curve Cryptography (ECC) to address the unique challenges posed by the IoT ecosystem. Implemented within the MATLAB environment, our approach offers a novel solution that combines the decentralized and immutable nature of blockchain with the efficiency and cryptographic security of ECC. The framework has been demonstrated to effectively enhance the security of IoT devices, ensuring their authenticity and the integrity of their data in a scalable and efficient manner. The adoption of blockchain technology in IoT security not only mitigates traditional cybersecurity risks but also introduces a new paradigm for building trust in decentralized device networks. Our MATLAB-based simulation serves as a practical tool for exploring the application of blockchain in IoT, offering insights into the design, implementation, and operation of secure IoT systems.

**FUTURE SCOPE:**

Looking ahead, several avenues for further research and development are evident:

* **Optimization for Resource Constrained Devices:** While ECC provides a balance between security and computational efficiency, further optimizations are necessary for deployment on the most resource constrained IoT devices. Research into lightweight cryptographic protocols and algorithms will be essential.
* **Dynamic and Scalable Consensus Mechanisms:** The current framework can benefit from the exploration of more dynamic consensus mechanisms that are scalable and energy-efficient, suitable for the vast and ever-changing landscape of IoT devices.
* **Cross-Chain Interoperability:** As IoT ecosystems often operate in siloed environments, developing standards and protocols for cross-chain interoperability could enhance the scalability and flexibility of IoT networks, enabling secure and seamless data exchange across different blockchain platforms.
* **Privacy-Preserving Techniques:** Integrating advanced privacy preserving techniques, such as zero-knowledge proofs, into the blockchain framework could further enhance the security of IoT devices, ensuring data privacy without compromising on transparency or integrity.
* **Real-World Implementation and Testing:** Moving beyond simulations, there is a critical need for real-world implementations and extensive testing of blockchain-based IoT security frameworks.

In conclusion, the integration of blockchain technology into IoT security presents a promising path forward in addressing some of the most pressing security challenges faced by IoT ecosystems today. By continuing to explore and develop these technologies, we can unlock the full potential of IoT, creating more secure, efficient, and trustworthy systems for the future.

# CHAPTER 10 REFERENCES

**CHAPTER 10 REFERENCES**

1. Lau, J. T. F., & Yeung, C. K. (2022). Blockchain-Based Authentication in IoT Networks. Semantic Scholar.
2. Zhang, Y., & Wen, Q. (2022). Blockchain-Based Secure Authentication with Improved Performance for Fog Computing. IEEE Access, 10, 109203-109216.
3. Ali, M. S., & Lee, S. (2023). Blockchain-Inspired Lightweight Authentication Protocol for IoT Networks. Electronics, 12(4), 867.
4. Liu, Y., Lu, Q., Chen, S., Qu, Q., O’Connor, H., Raymond Choo, K. K., & Zhang, H. (2020).

Capability-based IoT access control using blockchain. Digital Communications and Networks, 7(4), 463-469.

1. Qu, C., Tao, M., & Yuan, R. (2018). A hypergraph-based blockchain model and application in internet of things-enabled smart homes. Sensors, 18(9), 2784.
2. Maitra, S., Yanambaka, V. P., Abdelgawad, A., Puthal, D., & Yelamarthi, K. (2020). Proof-of Authentication Consensus Algorithm: Blockchain-based IoT Implementation. IEEE Access, 8, 156625-156634.
3. Ngubo, C., Dohler, M., & Mcburney, P. (2019). Blockchain, IoT and sidechains. Lecture Notes in Electrical Engineering, 2239, 136-140.
4. Gong, X., Liu, E., & Wang, R. (2020). Blockchain-based iot application using smart contracts: Case study of M2M autonomous trading. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15-18 May 2020, pp. 781-785.
5. Alrehaili, A., & Mir, A. (2020). POSTER: Blockchain-based Key Management Protocol for Resource-Constrained IoT Devices. In Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 3-5 November 2020, pp. 253-254.
6. Zhang, Y., & Wen, Q. (2021). A Blockchain-based Dynamic Access Control Scheme for IoT Networks. IEEE Internet of Things Journal, 8(12), 8957-8967.
7. Li, Y., & Liu, J. (2020). A Blockchain-based Trust Management Scheme for IoT. IEEE Access, 8, 110183-110194.
8. Zhang, Y., & Wen, Q. (2022). Blockchain-Based Authentication and Access Control for IoT
9. Chen, Y., & Liu, Y. (2020). A Blockchain-based Authentication and Authorization Framework for IoT. IEEE Access, 8, 167463-167475.
10. Zhang, Y., & Wen, Q. (2021). A Blockchain-Based Secure Data Sharing Scheme for IoT. IEEE Access, 9, 116114-116126.
11. Zhang, Y., & Wen, Q. (2021). A Blockchain-Based Secure and Decentralized Resource Management Scheme for IoT. IEEE Access, 9, 117498-117511

# FUNDING AND PUBLISHED PAPER DETAILS

We have applied for KSCST project funding on 10th February 2024. The corresponding details and proof of application has been attached in the below link.

https://drive.google.com/file/d/1poIrf9OwUgIp\_lDman2rB7oJEafkM5- V/view?usp=sharing

The codes, input files, output files and the report is uploaded to the following Git hub link mentioned below.

https://github.com/Dhanunjay-Raparla/Urban\_Flood\_Assessment\_and\_Evaluation

# APPENDIX - 1

2

ORIGINALITY REPORT

%

SIMILARITY INDEX

1%

INTERNET SOURCES

1%

PUBLICATIONS

1%

STUDENT PAPERS

PRIMARY SOURCES

1 Logan Widick, Ishan Ranasinghe, Ram Dantu, Srikanth Jonnada. "Blockchain Based

Authentication and Authorization Framework for Remote Collaboration Systems", 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2019

1%

Publication

1%

2 Submitted to The University of the West of Scotland

Student Paper

1

dergipark.org.tr

Internet Source %

3

Exclude quotes On Exclude bibliography On