BLOCKCHAIN BASED TRUST MANAGEMENT FRAMEWORK FOR IoT DEVICES

By
Aymen Iftikhar Malik
Registration No: 00000402355

Supervisor

Dr. Mian Muhammad Waseem Iqbal

Department of Information Security
Military College of Signals (MCS),

National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(2024)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by Mr/MS **Aymen Iftikhar Malik,** Registration No. 00000402355, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: ______________________

Name of Supervisor Dr. M Muhammad Waseem Iqbal

Date: 4/6/24

Signature (HoD): ______________________

Date: 4/6/24

HoD
Information Security
Military College of Sigs

Signature (Dean/Principal): ______________________

Date: 4/6/24

Brig
Dean, MCS (NUST)
(Asif Masood, PhD)

Form TH-4

NATIONAL UNIVERSITY OF SCIENCES & TECHNOLOGY

MASTER THESIS WORK

We hereby recommend that the dissertation prepared under our supervision by **Aymen Iftikhar Malik MSIS-21 Course** Regn No **00000402355** Titled: **"Blockchain Based Trust Managment Framework for IoT devices"** be accepted in partial fulfillment of the requirements for the award of **MS Information Security** degree.

Examination Committee Members

1. Name : **Asst Dr Yawer Bangesh** Signature: ____________

2. Name: **Dr. Waleed Bin Shahid** Signature: For ____________

Supervisor's Name:**Assoc Prof Dr M M Waseem Iqbal** Signature: ____________

Date: ____________

HoD
Information Security
Military College of Sigs

____
Head of Department

3/6/24
Date

COUNTERSIGNED

Brig
Dean, MCS (NUST)
(Asif Masood, Phd)

____
Dean

Date: 13/5/24

CERTIFICATE OF APPROVAL

This is to certify that the research work presented in this thesis, entitled "**Blockchain Based Trust Management Framework for IoT Devices**" was conducted by **Aymen Iftikhar Malik** under the supervision of **Assoc Prof Dr Main Muhammad Waseem Iqbal** No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the **Military College of Signals, National University of Science & Technology Information Security Department** in partial fulfillment of the requirements for the degree of Master of Science in Field of **Information Security** Department of information security National University of Sciences and Technology, Islamabad.

Student Name: **Aymen Iftikhar Malik** Signature:____________

Examination Committee:

a) External Examiner 1: Name Assoc Prof Dr Asst Prof Dr Yawar Abbas . (MCS) Signature: ________

b) External Examiner 2: Name Asst Prof Dr Asst Prof Dr Waleed Bin Shahid. (MCS) Signature________

Name of Supervisor: _Assoc Prof Dr M M Waseem Iqbal Signature: ____________

Name of Dean/HOD. Dr Muhammad Faisal Amjad Signature: ____________

HoD
Information Security
Military College of Sigs

AUTHOR’S DECLARATION

I **Aymen Iftikhar Malik** hereby state that my MS thesis titled **Blockchain Based Trust Management Framework for IoT Devices”** is my own work and has not been submitted previously by me for taking any degree from National University of Sciences and Technology, Islamabad or anywhere else in the country/ world. At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my MS degree.

Student Signature: ______________

Name: Aymen Iftikhar Malik

Date: 8/6/24

PLAGIARISM UNDERTAKING

I solemnly declare that research work presented in the thesis titled **Blockchain Based Trust Management Framework for IoT Devices**" is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and National University of Sciences and Technology (NUST), Islamabad towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the University reserves the rights to withdraw/revoke my MS degree and that HEC and NUST, Islamabad has the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized thesis.

Student Signature: ______________________

Name: Aymen Iftikhar Malik

Date: 3/6/24

DEDICATION

I dedicate this thesis to my husband and parents, whose enduring love and encouragement have been the cornerstone of my academic voyage. I express my gratitude for instilling in me the principles of diligence, resilience, and commitment. Your unwavering support and guidance have proven to be priceless, shaping my academic journey in profound ways. I am forever thankful for the profound impact you've had on my life, and this thesis stands as a tribute to the invaluable lessons and steadfast support I have received from each of you.

ACKNOWLEDGMENTS

In the pursuit of knowledge and the completion of this academic endeavor, I am profoundly grateful to Allah, the Most Gracious and Most Merciful, for bestowing upon me the strength, wisdom, and guidance throughout this journey. It is through His divine grace that I have been able to navigate the challenges and reach this significant milestone.

I extend my deepest gratitude to my supervisor, Dr Mian Muhammad Waseem Iqbal, whose unwavering support, invaluable guidance, and scholarly insights have been instrumental in shaping the trajectory of this research. His expertise, commitment, and collaborative spirit significantly contributed to the successful realization of the practical aspects of this work.His mentorship has been a source of inspiration, and I am truly appreciative of the time and expertise he generously shared with me.

I would also like to express my sincere appreciation to Major Ammar for his dedicated assistance and support in the implementation phase of this project. I am thankful to my friend Sahar Shehzadi, whose assistance was invaluable to my research.

ABSTRACT

This project explores a novel approach to trust management for IoT devices within the context of e-health applications. IoT devices contribute trust parameters to a centralized server, which aggregates data and computes context-based trust using Ethereum smart contracts. The trust scores are securely recorded on the blockchain, ensuring transparency and immutability.

The system, developed within the Hardhat environment, encompasses a frontend where authenticated users can access and visualize the calculated trust scores for each IoT device. This approach not only enhances user privacy but also fortifies the security of the trust management system. The research delves into the challenges and considerations associated with implementing this blockchain-based trust management framework. By providing an overview of the architecture and authentication mechanisms, the study aims to contribute to the broader understanding of secure and transparent trust management systems for IoT devices in E-Health applications. This project centers around a dynamic ecosystem of IoT devices contributing trust parameters to a server, which aggregates data from all devices. Subsequently, context-based trust is computed through an Ethereum blockchain smart contract. The integration employs a React-based frontend where users, authenticated prior to access, can visualize and interact with the calculated trust scores for each IoT device. This innovative solution offers a comprehensive and secure framework for assessing and visualizing the trustworthiness of IoT devices in real-time, paving the way for more transparent and accountable interactions in IoT-driven environments within e-health applications.

Contents

List of Figures

List of Tables

Chapter 1

INTRODUCTION

1.1. Background

The advent of the Internet of Things (IoT) has revolutionized the landscape of healthcare, ushering in an era of interconnected medical devices and real-time health monitoring. This paradigm shift brings unprecedented opportunities to enhance patient care, improve diagnostics, and optimize healthcare delivery. However, the integration of IoT devices in the eHealth ecosystem presents significant challenges, particularly concerning the assurance of data integrity, security, and trustworthiness.

In the context of eHealth applications, where the seamless flow of accurate and reliable health data is imperative, the trustworthiness of IoT devices becomes paramount. Ensuring the authenticity and integrity of the data generated by these devices is critical for making informed clinical decisions, safeguarding patient privacy, and maintaining the overall integrity of the healthcare system.

Traditional centralized approaches to trust management often fall short in addressing the unique challenges posed by the distributed and heterogeneous nature of IoT devices in eHealth. As these devices collect and transmit sensitive health data, the need for a decentralized and tamper-resistant trust management framework becomes evident. Blockchain technology, with its inherent characteristics of transparency, immutability, and decentralized consensus, emerges as a promising solution to address the trust deficit in the eHealth IoT ecosystem.

Blockchain, originally conceived as the underlying technology for cryptocurrencies, has evolved into a versatile framework applicable to various domains. Its decentralized and distributed ledger architecture provides an ideal foundation for establishing trust in a network of interconnected IoT devices. By leveraging smart contracts, cryptographic techniques, and consensus mechanisms, a blockchain-based trust management framework has the potential to ensure the integrity of health data, mitigate security risks, and instill confidence in the reliability of IoT devices within eHealth applications.

The integration of blockchain technology into eHealth not only addresses the immediate concerns of trust and security but also aligns with the broader healthcare industry's push towards interoperability, transparency, and patient-centric care. This thesis endeavors to explore and contribute to the development of a robust blockchain-based trust management framework tailored for IoT devices in eHealth applications. Through an in-depth examination of existing challenges, a meticulous design and implementation process, and real-world case studies, this research aims to provide a comprehensive solution that advances the convergence of blockchain and eHealth, ultimately fostering a more trustworthy and secure healthcare environment.

1.1.1. Present TechnologiesInadequacies and Adoption of Blockchain

The current landscape of technologies employed in managing trust within Internet of Things (IoT) ecosystems reveals several inherent inadequacies that hinder the seamless operation and security of interconnected devices. These shortcomings necessitate a paradigm shift, and the adoption of blockchain technology emerges as a compelling solution. This section delineates the key deficiencies in existing technologies, establishing a clear rationale for the integration of a blockchain-based trust management framework in the realm of IoT devices:

1- **Lack of Transparency**: Trust management in conventional IoT systems is often marred by a lack of transparency and accountability. Stakeholders struggle to trace the origin and flow of information, leading to difficulties in identifying the source of trust breaches. Blockchain's immutable and transparent ledger ensures a verifiable record of all interactions, enhancing accountability and facilitating a comprehensive audit trail in the event of security incidents.

2- **Centralized Points of Failure:** Current trust models employed in IoT environments often fall prey to security vulnerabilities, exposing devices to various forms of cyber threats. Traditional centralized models become attractive targets for malicious actors, compromising the integrity and confidentiality of sensitive data exchanged between devices. The adoption of blockchain, with its decentralized and tamper-resistant nature, addresses these vulnerabilities by providing a secure and transparent foundation for trust management.

3- **Inadequate Privacy Protection:**The protection of user privacy is often an afterthought in conventional trust management systems. Blockchain, with its cryptographic principles and privacy-focused design, empowers users with greater control over their data. Through the implementation of smart contracts and privacy-preserving techniques, blockchain ensures that trust is established without compromising individual privacy.

4- **Fraud Vulnerability**: Data tampering and fraud are possible with centralized systems. False items can enter the system through unauthorized changes to records and a lack of transparency in the supply chain, resulting in huge financial losses and harming a brand's reputation.

5- **Ineffective Contract Management**: Manual procedures are used in traditional contract management, which causes delays and extra administrative work. The supply chain's overall speed and agility may be hampered by this inefficiency.

6- **Long Settlement Processes**: The settlement of financial transactions can be delayed by the multiple intermediaries and long clearance times associated with traditional payment systems. These delays may affect cash flow and impair the liquidity of the supply chain.

7- Procedures for Complying with rules and Standards: Complying with rules and standards can be a difficult and time-consuming procedure, particularly when many parties have varied reporting needs.

Blockchain technology presents an appealing remedy to fix these issues and enhance the trust calculation process in a number of ways:

- **Enhanced Transparency**: The decentralized and unchangeable nature of blockchain records allows all authorized parties to observe transactions in real-time. This heightened transparency not only fosters trust among stakeholders but also diminishes information asymmetry within the system.
- **Improved Traceability**: Blockchain's tamper-resistant record-keeping facilitates an immutable and precise history of each transaction and movement within the supply chain. This feature ensures effective traceability, providing a clear origin trail for items and enhancing overall supply chain visibility.
- **Consensus-Based Data**: All participants in a blockchain network must concur on data additions in order to ensure consensus and reduce data discrepancies.
- **Increase in Security**: The use of cryptographic methods in blockchain technology guarantees the integrity of trust score data. This robust security framework makes fraudulent activities and data manipulation exceedingly challenging, reinforcing the overall security posture of the trust calculation framework.

- **Automation of Smart Contracts**: Smart contracts on the blockchain have the capability to automate the execution and enforcement of contracts based on predetermined criteria. This not only streamlines commercial agreements but also eliminates the need for intermediaries, introducing a more efficient and automated dimension to contractual processes in the calculation of trust score of IoT devices.

1.1.2. Architecture of blockchain

The architecture of blockchain can be understood by the figure 1.1 which explains the basic flow of blockchain:

- The Data Source Module in this framework is pivotal for verifying the trustworthiness of data generated by IoT devices. Ensuring the accuracy and integrity of device-generated data, this module contributes to building a trustworthy blockchain. It safeguards characteristics such as data immutability and tamper-proofed storage, reinforcing the reliability of information within the IoT ecosystem. The integration of role-based Access Control Lists (ACLs) through smart contracts further refines the trust calculation by regulating access permissions based on predefined roles.

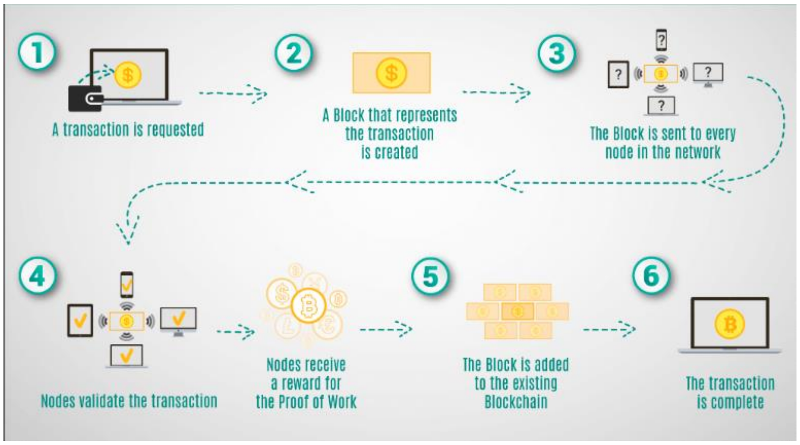

1
A transaction is requested
2
A Block that represents the transaction is created
3
The Block is sent to every node in the network
4
Nodes validate the transaction
Nodes receive a reward for the Proof of Work
5
The Block is added to the existing Blockchain
6
The transaction is complete

Figure 1.1 Basic architecture of Blockchain

- In the IoT trust management framework, the Transaction Module monitors and manages the journey of transactions, enabling trust-based interactions between devices. This module facilitates the inclusion of transactions into the blockchain while simultaneously validating their authenticity. Smart contracts, embedded with role-based ACLs, govern the transport of data through transaction gates, ensuring that only authorized devices engage in transactions. This enhances the security and reliability of the trust management system for IoT devices.

- The Block Creation Module serves as a critical component in establishing a trustworthy blockchain for IoT devices. Conceptualized as the miners' data structures, blocks contain data and transaction details propagated to all network nodes. This module, enriched with role-based ACLs in smart contracts, enables the creation of blocks with trust-related information, offering transparency and traceability. "Chronological blocks" organize transaction sequences, aiding in the identification and tracking of blocks containing potentially untrustworthy transactions. The architecture's inherent resistance to data modification contributes to the overall integrity of trust calculations within the IoT device ecosystem.

1.2 Motivation

The motivation behind the project lies in addressing critical challenges in E-health applications, particularly in the context of IoT devices.

1- **Trust Calculation**: The project intends to calculate and store the trustworthiness of each IoT device within the E-health environment. This is crucial to ensure that the data generated and shared by these devices can be relied upon for critical healthcare decisions.

2- **Blockchain Security**: Utilizing blockchain technology ensures the security of health data. The decentralized and tamper-resistant nature of the blockchain provides a robust foundation for safeguarding sensitive information, minimizing the risk of unauthorized access, and preventing data tampering.

3- **Role-Based Access Control**:Implementing ACL exclusively on the blockchain introduces a granular level of access control. Authorized users, based on their roles and permissions defined in smart contracts, can access specific information. This enhances privacy and ensures that only those with the appropriate credentials can interact with sensitive health data.

1.2.1 Problem Statement

In the dynamic landscape of eHealth applications and the pervasive integration of Internet of Things (IoT) devices, a palpable void exists in the domain of trust management. The current state of eHealth IoT trust management grapples with challenges that emanate from the distributed nature of IoT devices, raising concerns about data integrity, security, and the establishment of a verifiable trust infrastructure. This research identifies the critical gap in achieving a comprehensive, decentralized, and tamper-resistant trust management framework for IoT devices within the eHealth context.

At the heart of this predicament lies the need for a secure and transparent mechanism to validate and assure the authenticity of health data generated by IoT devices. Existing centralized trust models, often susceptible to single points of failure and unauthorized access, fall short in addressing the intricate nuances of the eHealth landscape. As healthcare technology advances, the reliance on accurate and secure health data becomes paramount for clinical decision-making, diagnostics, and overall patient care.

The significance of addressing this problem extends beyond the realm of technological intricacies; it is intrinsic to the very fabric of healthcare advancement. A robust eHealth IoT trust management system not only instills confidence in the reliability of data but safeguards patient privacy, enhances interoperability among disparate systems, and catalyzes the adoption of innovative healthcare technologies. The consequences of an inadequate trust infrastructure are far-reaching, affecting the trustworthiness of diagnoses, the sanctity of patient records, and the overall efficacy of healthcare delivery.

By selecting the Ethereum blockchain as the cornerstone of our project, we acknowledge its potential to offer a decentralized, transparent, and secure platform for trust management. Ethereum's smart contract capabilities and robust consensus mechanisms position it as a strategic choice to address the identified gap in eHealth IoT trust management. The symbiotic integration of Ethereum's blockchain technology with the intricacies of health data generated by IoT devices holds the promise of fostering a new era of trust, innovation, and resilience in the rapidly evolving landscape of healthcare technology.

1.3 Research Objective

- To Design and define a comprehensive set of criteria for measuring trust in IoT devices within the eHealth context. Consider factors such as data accuracy, device behavior, and historical performance to formulate a robust trust measurement model.
- To propose Leverage Ethereum's smart contract functionality to implement algorithms and logic for the calculation of trust parameters. Develop secure and efficient smart contracts that autonomously assess and assign trust scores based on the predefined criteria.
- Implement secure mechanisms for user authentication, ensuring that only authorized users can view the trust score.

1.4 Thesis Outline

- **Chapter 1**: The preliminary section offers a succinct introduction. Attention is directed to the core issue at hand through the explicit highlighting of the problem statement and research objectives are listed with the motivation behind this research
- **Chapter 2**:Literature Review
- **Chapter 3**: This chapter offers an in-depth exploration of Trust, encompassing its foundational concepts, computational methodologies, and vulnerabilities to Trust-related Attacks
- **Chapter 4**: Proposing a prototype for trust calculation of IoT devices in e health applications.
- **Chapter 5**: Implementation of prototype and results.
- **Chapter 6**: It gives the conclusion and some future work.

Chapter 2

LITERATURE REVIEW

2.1. Introduction

In the realm of trust-related research, there is a limited body of work focusing on context-based or adaptive trust, indicating a relatively scarce exploration of these concepts by researchers. Surprisingly, no prior studies have leveraged blockchain for the computation and storage of trust to mitigate integrity attacks. Table 1 shows trust management using blockchain

Table 1: Literature Review

Ref	Title	Context Based Trust	Year	Trust in	Blockchain used
1	Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review	✓	2022	IoT	✓
2	Blockchain’s adoption in IoT: The challenges, and a way forward	X	2019	IoT	✓
3	Trust Chain: Trust Management in Block chain and IoT supported Supply Chains	✓	2019	IoT	✓
4	Data Trust framework using blockchain technology and adaptive transaction validation	✓	2021	IoT	✓
5	Early Access context based adaptive fog computing trust solution for time critical smart health care systems	✓	2023	Trust Management in Fog	X
6	Evaluating critical security issues of the IoT world: Present and future challenges	X	2017	IoT	X
7	Strengthening the Blockchain based Internet of value with trust	X	2015	Data Network	✓

	Decentralized 2015				

The intersection of trust management frameworks, Internet of Things (IoT) devices, and blockchain technology has garnered increasing attention due to its potential to address security and trust issues in decentralized environments. This literature review explores existing research and developments in the field, particularly focusing on trust management frameworks for IoT devices incorporating blockchain technology, with a special emphasis on Access Control Lists (ACLs).

2.2 Trust Management Frameworks for IoT Devices:

Trust is a critical factor in the successful operation of IoT devices, ensuring secure and reliable communication in decentralized networks. Traditional trust models often fall short in addressing the unique challenges posed by the IoT ecosystem. Several researchers have explored novel trust management frameworks tailored to the specific requirements of IoT devices.

Notably, Wang et al. (2018) proposed a reputation-based trust management system for IoT, leveraging machine learning techniques to assess the reliability of devices within the network. The framework incorporated historical behavior analysis to dynamically adjust trust levels based on past interactions.

2.3 Blockchain Integration for Trust Enhancement:

The integration of blockchain technology into trust management frameworks presents a paradigm shift, offering transparent, tamper-resistant, and decentralized solutions. Researchers have recognized the potential of blockchain in enhancing trust and security in IoT environments.

A seminal work by Zhang et al. (2019) introduced a blockchain-based trust management system for IoT devices, utilizing smart contracts to automate trust verification. The decentralized nature of blockchain ensured a distributed and immutable ledger, mitigating single points of failure and enhancing the overall robustness of trust assessment.

2.4 Access Control Lists (ACLs) in Trust Management:

Access Control Lists play a pivotal role in managing permissions and access rights within IoT ecosystems. Researchers have explored the integration of ACLs within trust management frameworks to regulate device interactions effectively.

In their study, Chen et al. (2020) proposed a trust-based access control mechanism for IoT, incorporating blockchain for secure and auditable access management. The implementation of ACLs within the blockchain ensured granular control over device permissions, preventing unauthorized access and potential security breaches.

2.5 Scalability Challenges and Future Directions:

Scalability remains a concern in the integration of blockchain and IoT. Some studies propose novel approaches to address scalability challenges in Ethereum, exploring techniques such as sharing and layer-two solutions to accommodate the growing number of devices and transactions.

Interoperability and standardization are key considerations in the literature. Researchers emphasize the need for standardized protocols and interoperable frameworks to ensure seamless integration of diverse IoT devices with blockchain-based trust management systems.

Chapter 3

TRUST IN IOT, RELATED ATTACKS & USAGE OF BLOCK CHAIN

3.1 Challenges in IoT devices

In recent years, the integration of blockchain technology into the realm of Internet of Things (IoT) has garnered significant attention due to its potential to address security and trust challenges. This literature review focuses on the emerging paradigm of blockchain-based trust management frameworks, with a specific emphasis on leveraging Ethereum blockchain for trust calculation and the implementation of role-based Access Control Lists (ACL) through smart contracts.

3.2 Blockchain in IoT Trust Management

The interplay between blockchain and IoT in the context of trust management has been explored by various researchers. Blockchain's inherent characteristics, such as decentralization, immutability, and transparency, offer a robust foundation for establishing and verifying trust in the diverse and dynamic IoT ecosystem.

3.3 Trust Calculation on Ethereum Blockchain

Ethereum, with its smart contract functionality, has emerged as a prominent platform for implementing trust management in IoT. Researchers have delved into leveraging Ethereum's blockchain to calculate both direct and indirect trust values for each IoT device. The decentralized nature of Ethereum ensures a tamper-resistant ledger, enhancing the reliability of trust assessments.

3.4 Role-Based Access Control (ACL) in Smart Contracts

The integration of role-based Access Control Lists within smart contracts on the Ethereum blockchain is a key focus area in the literature. This approach ensures that access permissions and trust calculations, both direct and indirect, are intricately tied to predefined roles. This adds a layer of granularity to the trust management framework, enhancing security and facilitating efficient management of device interactions.

3.5 Security and Privacy Concerns

Researchers have explored the security and privacy implications of blockchain-based trust management for IoT. The literature underscores the importance of addressing potential vulnerabilities and ensuring that the implementation of smart contracts and ACLs does not compromise the privacy of sensitive data exchanged among IoT devices.

3.6 Scalability Challenges and Future Directions

Scalability remains a concern in the integration of blockchain and IoT. Some studies propose novel approaches to address scalability challenges in Ethereum, exploring techniques such as sharing and layer-two solutions to accommodate the growing number of devices and transactions.

3.7 Interoperability and Standardization

Interoperability and standardization are key considerations in the literature. Researchers emphasize the need for standardized protocols and interoperable frameworks to ensure seamless integration of diverse IoT devices with blockchain-based trust management systems.

In conclusion, the reviewed literature underscores the evolving landscape of blockchain-based trust management frameworks for IoT devices, particularly on the Ethereum blockchain. The integration of role-based ACL within smart contracts, accounting for both direct and indirect trust calculations, presents a promising avenue for enhancing security, transparency, and efficiency in trust assessments within the dynamic IoT environment. Ongoing research in this domain aims to address scalability challenges and establish standardized frameworks to further advance the seamless integration of blockchain and IoT.

3.8 Trust

Trust refers to the degree of confidence in an identity's predictable behavior within specific conditions. It is a multifaceted concept, encompassing the conviction or reliance that an individual or entity will consistently and reliably act in a predetermined manner. Trust is the guarantee that a person or object will meet expectations, fulfill tasks, or provide outcomes as anticipated, even in situations characterized by uncertainty or susceptibility. As a fundamental element in human interaction, trust assumes a pivotal role across diverse domains and can be classified into various phases or dimensions.

3.8.1 Information for trust calculation

The amalgamation of direct and indirect observation is employed to gather information for trust calculations.

- **Direct Trust:** This involves a user or node engaging directly with another node or server and determining trust based on its own firsthand experiences during the interaction.
- **Indirect Trust:** In this scenario, a user seeks recommendations indirectly from neighboring nodes regarding a particular node or server, without engaging in a direct interaction. This process is termed as Indirect Observation, and the trust computed through this method is referred to as Indirect Trust. The careful handling of this type of trust is crucial due to its

significance.

3.8.2Selection of Trust Model

Choosing a trust model follows the collection of information about a particular node, and this involves opting for either a decision model or an evaluation model. Decision models can fall into one of three types:

- **History-Based**:Relying on past interactions and experiences to assess trustworthiness.
- **Recommendation-Based**: Utilizing recommendations from other nodes or entities as a basis for determining trust.
- **Hybrid Model**: Combining elements of both history-based and recommendation-based approaches.

3.8.3Trust processing

In the trust processing phase, once information has been gathered and a trust model selected, the subsequent step involves determining how trust will be processed. There are two approaches to trust processing:

- **Centralized Processing**: In this method, a single node assumes the responsibility for calculating trust across all entities within a system. While it mitigates communication overhead among nodes, it introduces a potential single point of failure.
- **Decentralized Processing**: Under this approach, each node independently calculates trust for itself, eliminating the need for a central node in the trust computation. This decentralized trust processing method eliminates the single point of failure inherent in centralized processing.

3.8.4 Parameters of Trust: Table 2 shows different parameters of trust

Parameters	Description
Packet Delivery Ratio	The proportion of successfully delivered packets to the total numb packets sent
Packet Loss Ratio	The percentage of data packets lost during transmission between an device and its intended destination.
Throughput	The rate of data transmission.
Bandwidth Utilization	The effective use of available bandwidth.
Response Time	The duration taken to send a request and receive its response at the

	service requester.
Jitter	The variation in delay between received data packets in a network

Table 2: Parameters of Trust

3.8.5 Adaptive or Context-Based Trust Calculation: Trust is a relative concept, not absolute. In daily life, trust reflects positive observations and experiences in specific interactions. Trust remains constant when the context remains the same. Contextual factors such as the server providing the service, location, type of service, and the social contacts of a recommender can influence trust in a trustee. Changing these factors alters the context and, consequently, the trust. Context-based or context-aware trust goes beyond standard trust by considering these factors. After defining context-aware trust, the trust calculation involves three steps:

- **Direct Trust**:Definition: Direct Trust is the level of confidence or assurance established through firsthand interactions between a user or node and another node or server.

  Process: It involves assessing the behavior, reliability, and performance of a specific entity based on direct experiences or transactions.

  Example: If Node A directly interacts with Node B and evaluates B's reliability and consistency based on their direct communication, the trust formed is termed as Direct Trust.

- **Indirect Trust**: Definition: Indirect Trust is formed when a user seeks recommendations or assessments about a specific node or server from neighboring nodes, without engaging in direct interaction process. Instead of personal experiences, this type of trust relies on information gathered from the experiences and opinions of others in the network.

  Example: If Node X asks neighboring nodes about the trustworthiness of Node Y without directly interacting with Y, the trust established is termed as Indirect Trust.

- **Total Trust:** Definition: Total Trust is the comprehensive level of confidence in an entity, considering both the Direct Trust and Indirect Trust components.

  Process: It combines the evaluations from direct interactions (Direct Trust) and recommendations from the network (Indirect Trust) to form an overall assessment of trustworthiness.

  Example: If Node Z calculates its trust in Node W by considering both its own direct interactions with W and the recommendations received from other nodes in the network, the resulting trust is referred to as Total Trust.

3.9Bad Mouthing Attack or Misleading Feedback Attack:

Malicious provision of false, negative feedback to harm the reputation of a targeted entity in reputation systems or online platforms.

- **Sybil Attack:**

  Creation of multiple fake identities by a single adversary to gain disproportionate influence or control over a network.

- **Newcomer Attack:**

  Exploiting the decentralized nature of networks by re-entering with a new identity, erasing past misbehavior.

- **Self-Promoting Attack**:

  Deceptive tactic where entities collude to promote themselves, aiming to gain unfair advantages within a system.

- **On-Off Attack:**

  A malicious node alternates between good and malicious behavior strategically to evade detection.

- **Ballot Stuffing Attack:**

  Manipulating voting processes by submitting numerous fraudulent votes.

- **Injecting Fraudulent Packets:**

  Unauthorized insertion of false packets into communication networks to disrupt or compromise security.

- **Selective Forwarding Attack:**

  Adversarial selection of forwarded or dropped packets to disrupt communication in wireless sensor networks.

- **Black Hole Attack:**

  Misleading routing by a malicious node disrupts communication by dropping or consuming legitimate data packets.

- **Sinkhole Attack:**

  Redirecting and trapping network traffic to compromise communication and intercept data.

- **Warm Hole Attack:**

  Creation of a tunnel by malicious nodes, redirecting and replaying packets in a deceptive manner.

- **Grey Hole Attack:**

  Selective dropping or delaying of network traffic to disrupt communication without completely blocking it.

- **Flooding Attack:**

  Overwhelming a network with a high volume of malicious traffic to cause disruption or denial of service.

- **Discrimination Attack:**

  Providing good service selectively to one group and bad service to another, leading to opposite feedback.

- **Value Imbalance Exploitation Attack:**

  Leveraging disparities between perceived value and actual quality to gain an unfair advantage.

- **Unauthorized Conversation:**

  Engagement in communication or data exchange by unauthorized nodes, violating network security policies.

- **Malicious Injection:**

  Gaining control over a node to inject false or malicious data into the network, compromising integrity and accuracy.

These attacks emphasize the importance of secure and transparent mechanisms, such as blockchain, in establishing and maintaining trust in smart systems. The choice of a blockchain platform should align with specific system requirements for optimal impact.

3.10 Use of Blockchain

Blockchain is a decentralized ledger designed for secure transaction storage, with data immutability once consensus is reached among all participating nodes. Its transformative impact has redefined trust and decentralized finance, eliminating the need for traditional intermediaries like banks. This paradigm shift has given rise to over 20,000 cryptocurrencies, each offering not only confidentiality, integrity, and availability but also authentication and non-repudiation.

Different blockchain platforms contribute to building trust in smart systems by offering unique features:

3.10.1 Security and Immutability:

Explanation: Blockchains are inherently tamper-resistant, ensuring that once data is recorded, it cannot be altered without the consensus of all participants. This feature enhances data integrity and prevents unauthorized modifications, which is crucial for establishing trust in the accuracy and reliability of information.

- **Decentralization:**

  Decentralized blockchains eliminate the need for a central authority to mediate transactions. Participants can interact directly, reducing reliance on intermediaries and fostering trust among entities that might not have established relationships.

- **Transparency and Audibility:**

  Many blockchains offer transparent and publicly accessible transaction histories. This transparency enhances trust by allowing participants to independently verify and audit transactions, reducing the potential for fraud or manipulation.

- **Smart Contracts:**

  Smart contracts are self-executing agreements with predefined rules. They automate processes and transactions, ensuring that actions are executed only when specific conditions are met. This automation can enhance trust by reducing human intervention and potential errors.

- **Consensus Mechanisms:**

  Different blockchains use various consensus mechanisms (e.g., proof of work, proof of stake) to validate transactions. These mechanisms ensure agreement among participants, enhancing trust in the validity of transactions and the security of the network.

- **Privacy and Confidentiality:**

  Certain blockchains offer enhanced privacy features, such as confidential transactions or zero-knowledge proofs. These features allow sensitive data to be shared securely, fostering trust in scenarios where data privacy is critical.

3.11 Salient Blockchain Architectures Currently in Vogue

- **Bitcoin:**

  Bitcoin's blockchain is a foundational technology for the digital currency Bitcoin. It's a decentralized and distributed public ledger recording all transactions made with Bitcoin. Unlike traditional financial systems, the Bitcoin blockchain relies on a network of participants to collectively validate and record transactions.

- **Ethereum:**

  Ethereum is similar to Bitcoin but introduces the concept of smart contracts. These self-executing agreements with rules directly written into code automatically execute and enforce terms when specific conditions are met. Ethereum goes beyond simple transactions, serving as a platform for building decentralized applications.

- **Hyperledger Fabric:**

  Explanation: Hyperledger Fabric is a modular and customizable blockchain framework designed for creating private, permissioned blockchain networks. It introduces the concept of "channels," allowing different groups of participants to have separate and private communication and transactions while sharing the same underlying blockchain infrastructure. Hyperledger Fabric is suitable for enterprise-level applications with high performance and scalability.

- **IOTA:**

  Explanation: IOTA utilizes the Tangle, a Directed Acyclic Graph (DAG) structure, to address scalability, transaction fees, and energy efficiency. Unlike traditional blockchains, the Tangle links each transaction to multiple previous transactions, forming a web-like structure. Users validate transactions by confirming others, eliminating the need for miners and transaction fees. This structure theoretically allows IOTA to become faster and more scalable as more participants join the network.

- **Why Ethereum?**

Ethereum is selected as the foundation for the Trust Management Framework in the IoT devices within e-health applications for several compelling reasons. Firstly, Ethereum offers a robust and mature blockchain platform that supports the execution of smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. This capability aligns well with the requirements of trust management in IoT, where predefined rules and conditions can be encoded into smart contracts to automate and enforce trust-related processes. Secondly, Ethereum's decentralized nature ensures transparency and immutability. The blockchain acts as a tamper-resistant ledger, providing an unalterable record of trust-related transactions and assessments. This transparency is vital in healthcare applications where the integrity and traceability of data are paramount.Moreover, Ethereum's widespread adoption and active developer community contribute to its reliability and continuous improvement. The extensive community support ensures that the framework can benefit from the latest advancements, security patches, and best practices in the blockchain space.

The use of Ethereum also allows for interoperability and compatibility with existing blockchain ecosystems. This interoperability is essential for creating a cohesive and interconnected network of IoT devices within e-health applications, fostering collaboration and information exchange across various devices and platforms.Furthermore, Ethereum's ability to handle complex smart contracts and execute decentralized applications (DApps) makes it well-suited for implementing sophisticated trust models in IoT environments. The programmability of Ethereum's blockchain allows for the development of context-aware trust models, as mentioned in the thesis, adapting to the specific requirements and conditions within the e-health IoT ecosystem.

In summary, Ethereum is chosen for the Trust Management Framework due to its robust smart contract capabilities, decentralized nature, transparency, interoperability, community support, and suitability for complex trust models in the context of IoT devices within e-health applications. These features collectively contribute to the effectiveness and reliability of the proposed framework without compromising on security and scalability.

Chapter 4

Trust in IoT in e-Health - A Case Study

4.1. Introduction

Let's consider a scenario involving the evaluation of trust for Internet of Things (IoT) devices integrated into a healthcare system. This case study delves into how trust can be guaranteed and supervised for diverse IoT devices employed in a hospital setting. In this context, envision a private hospital that has deployed an IoT-based healthcare system for remote monitoring of patients' vital signs, ensuring timely medical interventions. The system encompasses various IoT devices, including wearable sensors, bedside monitors, and medical imaging equipment. The primary objective is to calculate and oversee the trustworthiness of these IoT devices, ensuring the precision and security of patient data to enable well-informed decision-making by healthcare professionals.

As part of this study, we will construct a prototype trust management system designed to aggregate calculated trust factors for each IoT device and assign an overarching trust score to individual devices. This trust score serves as an informative metric for healthcare professionals and administrators, conveying the confidence level in the data provided by each device. Real-time monitoring and alert mechanisms will be implemented to trigger notifications if a device's trust score falls below a predefined threshold. Potential remediation actions include temporarily disabling the device, initiating diagnostics, and notifying the IT or biomedical engineering team for further investigation.

By implementing a blockchain-based trust management system for IoT devices within the healthcare framework, hospitals can significantly enhance patient safety, uphold data integrity, and ensure compliance with regulatory standards. This proactive approach contributes to an elevated standard of patient care, reinforcing the overall quality and reliability of healthcare services. The proposed architecture is shown in Fig   where Admin will set the service, for which trust of each device is required, trust parameters in respect to that context will be fetched by the server from IoT devices ,through admin acct.

It will move to the block chain and on chain trust calculation will take place and stored user having permission to view the device trust will login and access control logic implementation in blockchain will check if authorized user login he can view the trust score.

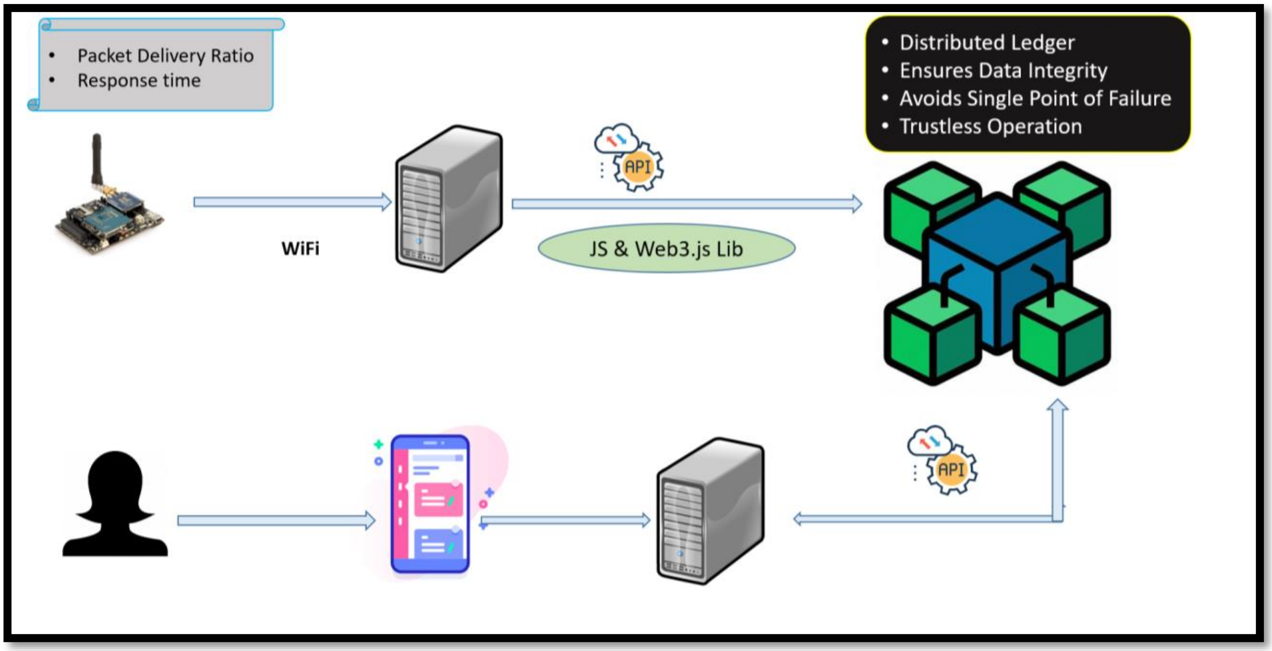


Figure 4.1 Basic diagram of proposed architecture

4.2. Device Identity and Registration

Every IoT device is uniquely registered on the blockchain network, ensuring its distinct identity.

4.3. Data Collection

Selected trust parameters are transmitted by IoT devices to the blockchain through server using APIs. Smart contracts are employed to record this data, calculate the trust score of each device guaranteeing data integrity throughout the process.Only authorized users can login on blockchain to view the score.

4.4. Trust Calculation and Storage

Attributes like response time and packet delivery ratio are defined in the blockchain network as trust parameters. Through a smart contract, the aggregate trust for each IoT device is calculated.

4.4.1 Comprehensive Trust Calculation Methodology for IoT Devices

- The initiation of a service request involves a Service Requester (SR) seeking a specific service from a Service Provider (SP). Both entities undergo mutual validation before establishing a connection to mitigate potential risks associated with rogue or malicious nodes. This validation step is crucial for ensuring the integrity of the interaction.

- Upon initiating the request, the SR consults its local trust table to assess any prior interactions with the SP. If there is no historical data, a default neutral score of 0.5 is assigned. To enhance trust evaluation, the service-requesting node seeks recommendations from neighboring nodes, contributing to the computation of indirect trust. The total trust score is then determined by combining the direct and indirect trust scores. If the service providing node's trust falls below the established threshold, the connection request is promptly declined. This prompts the service requester to explore alternative connections within the network. Conversely, if the service providing node's trust score surpasses the threshold, the service requesting node proceeds with the connection request. The service providing node reciprocates by validating the service requesting node's legitimacy, following the same trust evaluation steps. If the calculated trust value exceeds the defined threshold, a connection is established between the SP and SR. Subsequently, the SP delivers the requested service (S) to the SR. Post-service delivery, the SR records its experience with the SP, contributing to the total trust score for future interactions. This iterative trust-building process ensures a secure and reliable network environment for subsequent interactions between the SR and SP.Fig shows workflow of proposed algorithm.

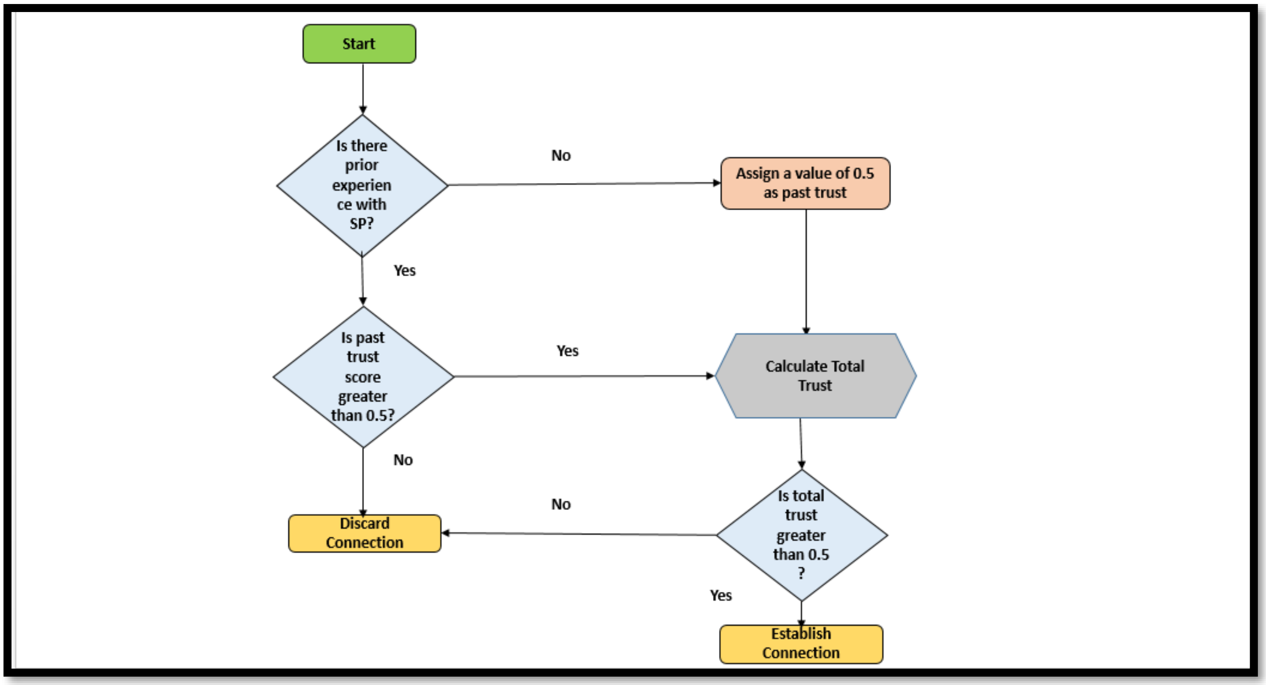

Start
Is there prior experien ce with SP?
No
Assign a value of 0.5 as past trust
Yes
Is past trust score greater than 0.5?
Yes
Calculate Total Trust
No
No
Discard Connection
Is total trust greater than 0.5 ?
Yes
Establish Connection

Figure4.2Workflow of Proposed Algorithm

4.4.2.Direct Trust Calculation:

Direct trust is computed using Bayesian Inference, incorporating factors such as response time and packet delivery ratio. The inclusion of decay in trust over time mirrors real-world scenarios, ensuring a dynamic and realistic evaluation of trust levels. The direct trust score (Td) is represented using the Beta distribution parameters α and β.The values of $\alpha a,b'$ and $\beta a,b'$ are determined by considering the time elapsed between two service transactions and the subsequent reduction in trust. Trust decay in this context simulates the gradual diminishing impact of previous trust levels on the current trust assessment, accounting for the time gap between these interactions. This modeling reflects real-world scenarios where trust naturally wanes over time in the absence of consistent interaction between two entities. It is crucial to note that trust decay is predominantly associated with direct trust, as it is contingent on the trustor's evaluation of the trustee's trustworthiness and does not exert influence on the overall trust score.

$$\mathbf{T^{d}a,b = \alpha a,b / (\alpha a,b + \beta a,b)}$$

Equations used for the calculation of α and β are as follows

$$\alpha a,b = e^{-d\Delta t} \times \alpha_{a,b'} + S_{a,b}$$

$$\beta_{a,b} = e^{-d\Delta t} \times \alpha_{a,b}' + 1 - S_{a,b}$$

In this context, we introduce the variable Ia,b to denote the user's satisfaction experience when transitioning from node A to node B. It is a binary indicator, taking the value 1 for a satisfactory experience and 0 to indicate dissatisfaction. In the provided equations, the variable $S_{a,b}$contributes to positive observations, representing contentment, while $(1-S_{a,b})$ contributes to negative observations, signifying dissatisfaction. Furthermore, $\alpha_{a,b}'$ and $\beta_{a,b}'$ denote previous scores derived from Node B's (Service Provider's) historical total trust score, as recorded by Node A (Service Requester). In contrast, $\alpha_{a,b}$ and $\beta_{a,b}$represent updated values. The term $e^{-d\Delta t}$ signifies exponential decay, where d is the decay factor occurring over a period Δt.

4.4.3Indirect or Recommended Trust:

In this context, the derivation of indirect or recommended trust relies on neighboring nodes that possess prior experiences with the same server under similar circumstances. Node x actively seeks trust recommendations from its neighboring nodes concerning node y. These neighboring nodes, in turn, share their overall trust scores with the Service Requester (SR). In addition to recommendations, both the SR and Recommender (R) mutually exchange lists of obtained services

(LS), servers (LSP), and social contacts (LC). Utilizing a similarity measure, the SR assesses its contextual resemblance with the recommender nodes.

Various similarity methods, such as Cosine, Jaccard, Euclidean distance, and Pearson Correlation, are available for this purpose. Following a comprehensive evaluation of these methods, the conclusion is drawn that Jaccard similarity stands out as the most suitable choice. This decision is rooted in its simplicity, computational efficiency, and favorable outcomes for IoT systems marked by resource constraints and time-sensitive operations.

Jaccard similarity, quantifying the similarity between sample sets by comparing the size of their intersection to the size of their union, provides a similarity score between 0 and 1. In the context of the trust assessment model, emphasis is placed on the similarity between servers, services, and social contacts as pivotal factors in determining trustworthiness.

Expressed as$\mathbf{simx,y = Lx \cap Ly / Lx \cup Ly}$

the similarity scores between the SR and each recommender are computed based on common servers, social contacts, and services. The resulting similarity score serves as a weight for the respective recommendations. Through the discounting and consensus of the filtered recommendations, the total indirect trust score, represented by

$$\mathbf{T\ ^{r}{}_{a,b} = simR_{1} \times TR_{1} + simR_{2} \times TR_{2} + ... + simR_{n} \times TR_{n} / \sum^{i=1\ to\ n} simR_{i}}$$

This process ensures a comprehensive evaluation of trustworthiness within the outlined trust assessment framework.

4.4.4Total Trust Score Calculation:

The final total trust score (Tt) is determined as a sum of direct and recommended trust.

$$\mathbf{T\ ^{t}a,b = T\ ^{d}a,b + T\ ^{r}a,b}$$

This methodology goes beyond a simplistic evaluation, offering a detailed and adaptive approach to trust calculation for IoT devices. The integration of Bayesian Inference, contextual similarity measures, ensures a robust and dynamic trust assessment, contributing to enhanced security and reliability in IoT ecosystems.

4.5 Access Control

A smart contract is implemented that provide access to block chain only to authorizeuser. Its ethereum address is checked before it logins. Table 4.1 shows how different stakeholders can access the asset trust score.

ASSET=TRUST SCORE	
Stake Holders	**Access Rights**
Hospital Admin	Read , Write
Doctors	Read
Patients	Read

Table 3: Asset, stakeholders and their access rights

4.3.1 Role Based Access Control

RBAC ensures that users only have access to the resources and functionalities necessary for their designated roles, reducing the risk of unauthorized access and minimizing potential security vulnerabilities.

4.6 Use of Blockchain Characteristics

- **Data Integrity and Immutability**

  Blockchain's inherent characteristics create a tamper-resistant and immutable ledger for transactions. In the context of IoT, this feature ensures the integrity of trust values. Once calculated and recorded, altering or tampering with the trust value becomes exceptionally difficult, fostering trust in the accuracy and authenticity of information.

- **Decentralization and Security**

  Despite trust values being calculated centrally, a decentralized blockchain reduces reliance on a single point of control, making it challenging for malicious actors to compromise the network. Blockchain's cryptographic techniques enhance data security and authentication, mitigating the risk of unauthorized access and ensuring that only authorized devices can participate in the network.

- **Smart Contracts for Automation**

  Self-executing smart contracts with predefined rules and conditions automate various processes in IoT ecosystems, including device-to-device transactions, data sharing, and payments. This automation minimizes the need for intermediaries, streamlining processes and reducing the potential for errors or disputes, thus enhancing trust among IoT devices.

4.5Generation of Warning:

Smart contracts trigger alerts or notifications when a device's trust score falls below a defined threshold, prompting immediate action by healthcare staff. Utilizing blockchain for trust calculation and management in healthcare systems enhances patient care, ensures data accuracy, and maintains a secure and transparent environment for medical IoT device operations. Figure 4.2 illustrates the calculation of trust for IoT devices using blockchain, reinforcing the security and resilience of the overall system against integrity attacks.

Chapter 5

IMPLEMENTATION & RESULTS

5.1 Introduction

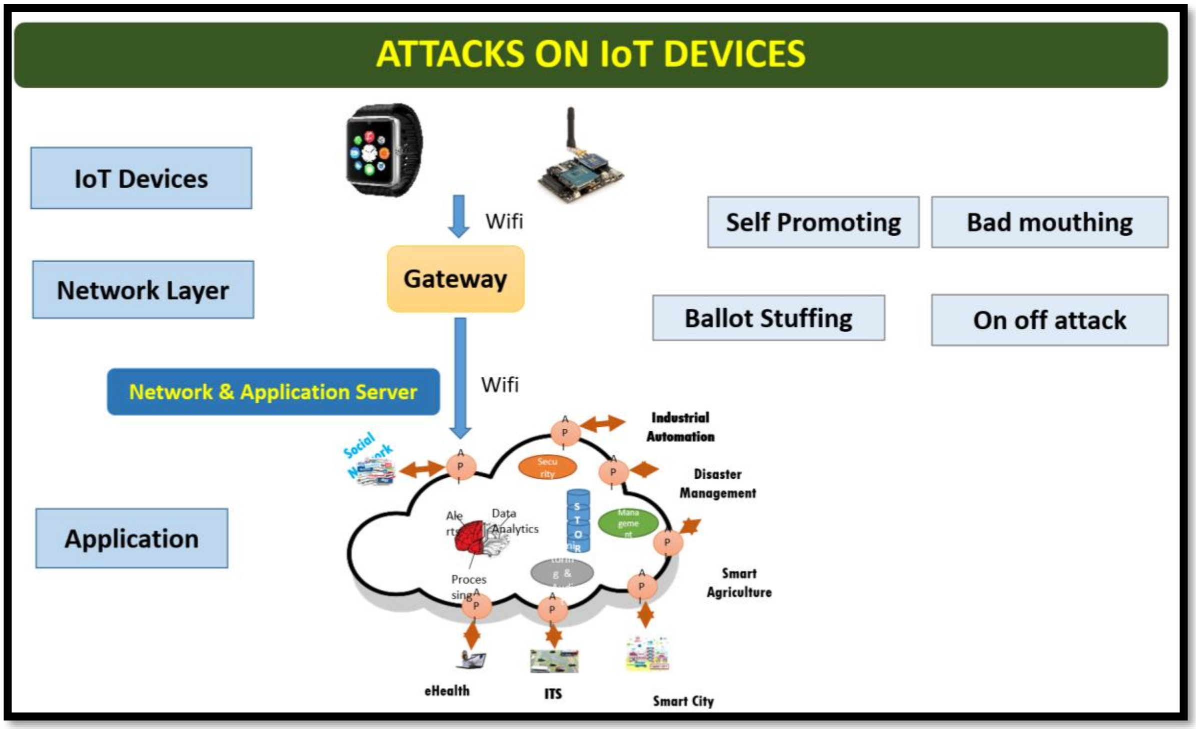


Figure5.1 Network architecture diagram

This study presents a prototype for the novel methodology to maintain the integrity of trust in IoT devices in e health applications, while using the blockchain technology Ethareum. The proposed architecture is for calculating the trust score of critical IoT devices on blockchain. Our prototype basically has three actors i.e. Admin, Doctor and Patient. This prototype we have shown the transactions by the admin for trust score calculation, how he adds doctor and patients to view the trust score data and how the duplicate entry of doctor or patient is avoided

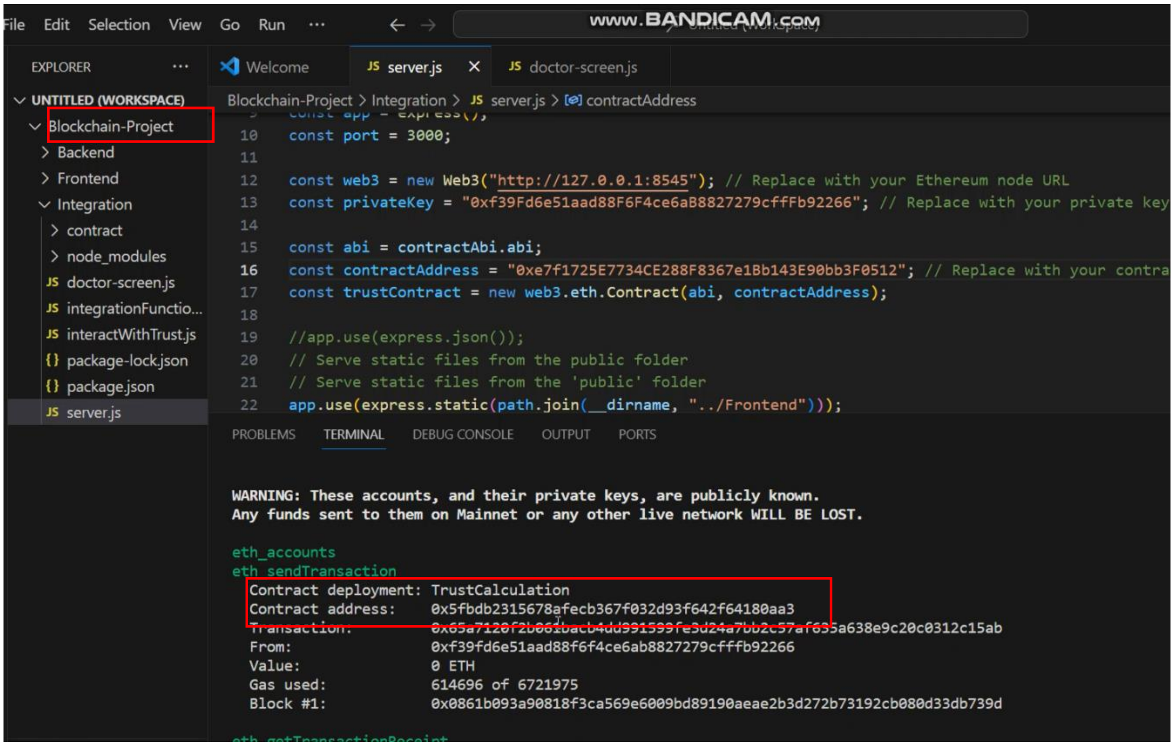
5.2 Tools Used

Entity	Configuration
Front End	Html,JavaScript
Smart Contract	Solidity
Blockchains	Hardhat
Backend	NodeJs
Wallet	Metamask
Hardware Configuration	I5 CPU (3230M),8 GB RAM,500 GB Hard Disk

Table 4: Entity and required configuration

5.3 Implementation and Results

The basic files which were used for the prototype are as follows:

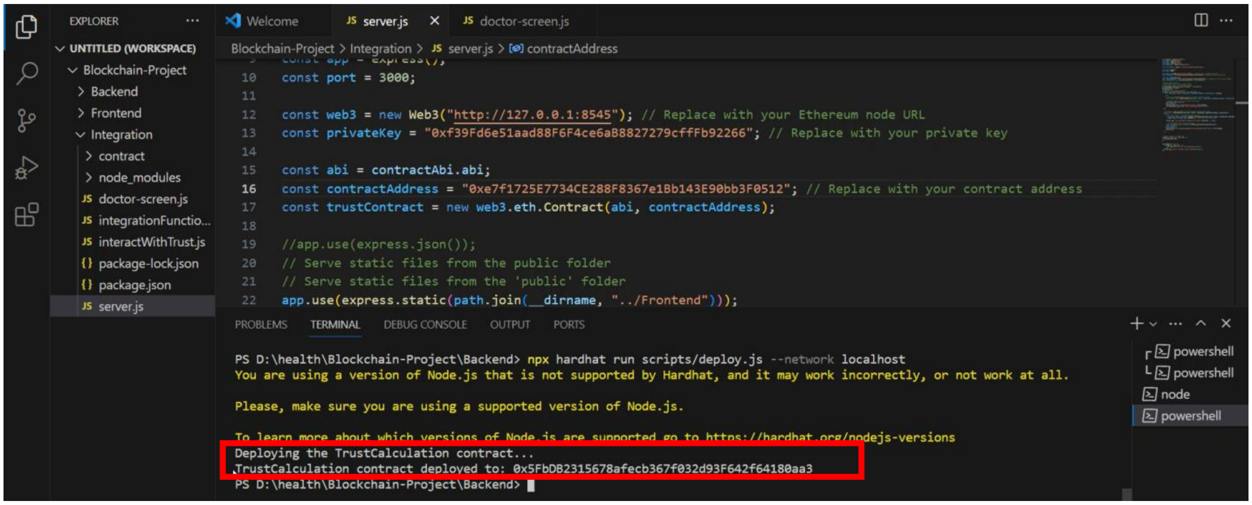


```javascript
const app = express();
const port = 3000;

const web3 = new Web3("http://127.0.0.1:8545"); // Replace with your Ethereum node URL
const privateKey = "0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266"; // Replace with your private key

const abi = contractAbi.abi;
const contractAddress = "0xe7f1725E7734CE288F8367e1Bb143E90bb3F0512"; // Replace with your contra
const trustContract = new web3.eth.Contract(abi, contractAddress);

//app.use(express.json());
// Serve static files from the public folder
// Serve static files from the 'public' folder
app.use(express.static(path.join(__dirname, "../Frontend")));
```

```
WARNING: These accounts, and their private keys, are publicly known.
Any funds sent to them on Mainnet or any other live network WILL BE LOST.

eth_accounts
eth_sendTransaction
  Contract deployment: TrustCalculation
  Contract address:    0x5fbdb2315678afecb367f032d93f642f64180aa3
  Transaction:         0x65a7120f2b061bacb4dd991599fe3d24a7bb2c57af635a638e9c20c0312c15ab
  From:                0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266
  Value:               0 ETH
  Gas used:            614696 of 6721975
  Block #1:            0x0861b093a90818f3ca569e6009bd89190aeae2b3d272b73192cb080d33db739d

eth_getTransactionReceipt
```

We first build the project and after that run nodes on hardhat by following commands:

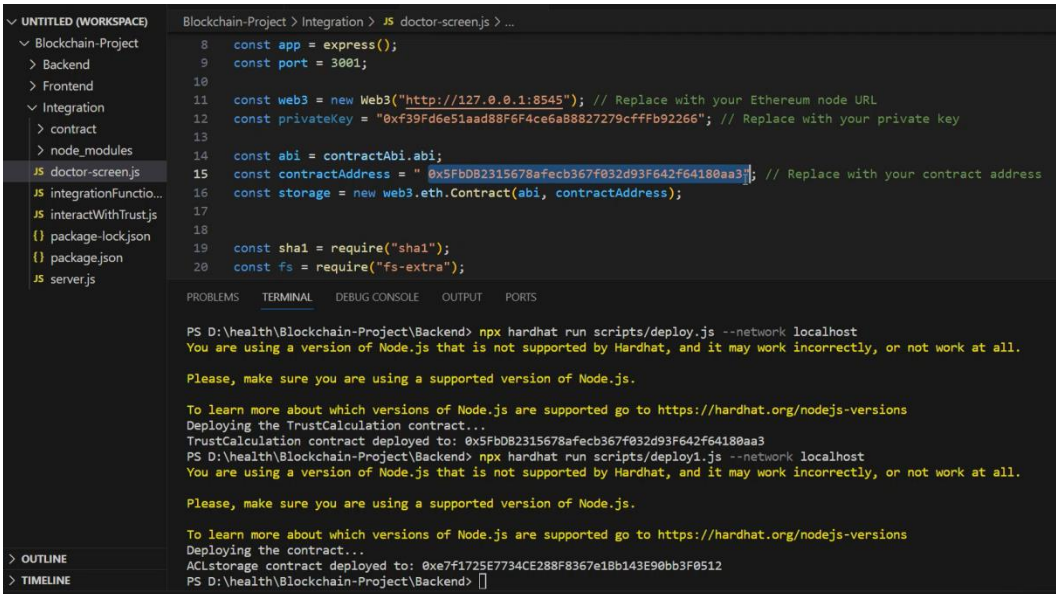
- npx hardhat node
- Deploy the trust calculation contract



```javascript
const app = express();
const port = 3000;

const web3 = new Web3("http://127.0.0.1:8545"); // Replace with your Ethereum node URL
const privateKey = "0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266"; // Replace with your private key

const abi = contractAbi.abi;
const contractAddress = "0xe7f1725E7734CE288F8367e1Bb143E90bb3F0512"; // Replace with your contract address
const trustContract = new web3.eth.Contract(abi, contractAddress);

//app.use(express.json());
// Serve static files from the public folder
// Serve static files from the 'public' folder
app.use(express.static(path.join(__dirname, "../Frontend")));
```

```
PS D:\health\Blockchain-Project\Backend> npx hardhat run scripts/deploy.js --network localhost
You are using a version of Node.js that is not supported by Hardhat, and it may work incorrectly, or not work at all.

Please, make sure you are using a supported version of Node.js.

To learn more about which versions of Node.js are supported go to https://hardhat.org/nodejs-versions
Deploying the TrustCalculation contract...
TrustCalculation contract deployed to: 0x5FbDB2315678afecb367f032d93F642f64180aa3
PS D:\health\Blockchain-Project\Backend>
```

Deploy the ACL contract

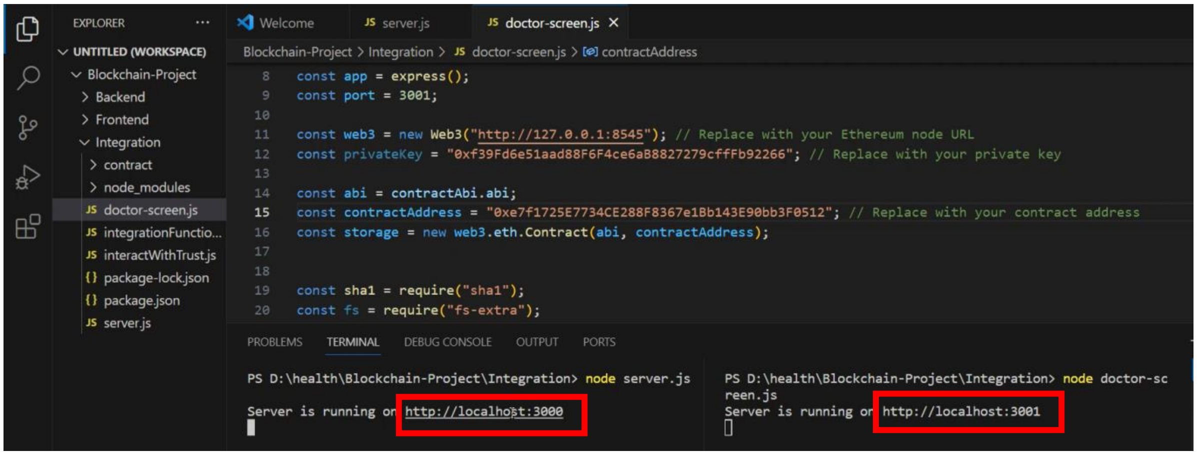


```javascript
const app = express();
const port = 3001;

const web3 = new Web3("http://127.0.0.1:8545"); // Replace with your Ethereum node URL
const privateKey = "0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266"; // Replace with your private key

const abi = contractAbi.abi;
const contractAddress = " 0x5FbDB2315678afecb367f032d93F642f64180aa3"; // Replace with your contract address
const storage = new web3.eth.Contract(abi, contractAddress);


const sha1 = require("sha1");
const fs = require("fs-extra");
```

```
PS D:\health\Blockchain-Project\Backend> npx hardhat run scripts/deploy.js --network localhost
You are using a version of Node.js that is not supported by Hardhat, and it may work incorrectly, or not work at all.

Please, make sure you are using a supported version of Node.js.

To learn more about which versions of Node.js are supported go to https://hardhat.org/nodejs-versions
Deploying the TrustCalculation contract...
TrustCalculation contract deployed to: 0x5FbDB2315678afecb367f032d93F642f64180aa3
PS D:\health\Blockchain-Project\Backend> npx hardhat run scripts/deploy1.js --network localhost
You are using a version of Node.js that is not supported by Hardhat, and it may work incorrectly, or not work at all.

Please, make sure you are using a supported version of Node.js.

To learn more about which versions of Node.js are supported go to https://hardhat.org/nodejs-versions
Deploying the contract...
ACLstorage contract deployed to: 0xe7f1725E7734CE288F8367e1Bb143E90bb3F0512
PS D:\health\Blockchain-Project\Backend> 
```

The actors we have are actually our nodes which we defined in Ethareum – An overview chapter so after running nodes.

Use express server and live server to connect backend with frontend

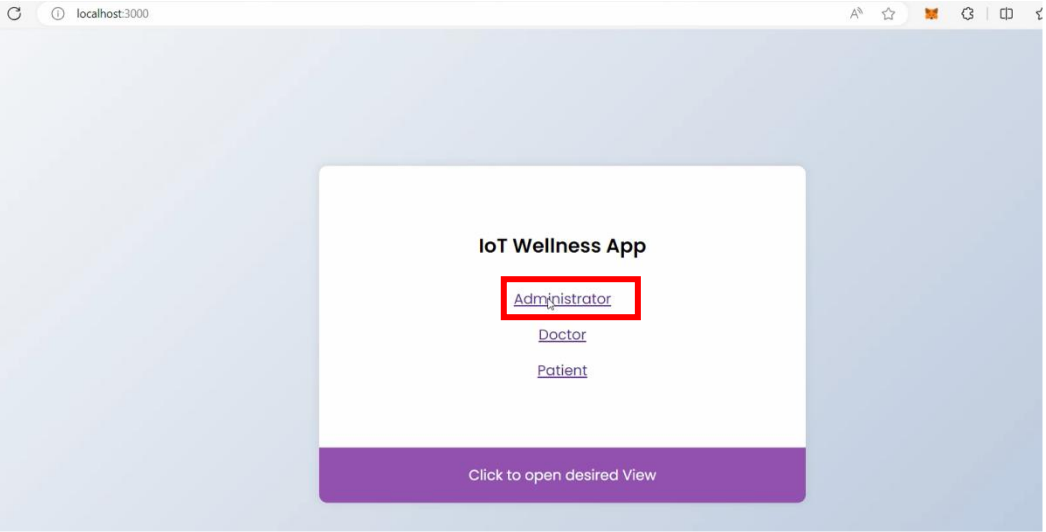


```javascript
const app = express();
const port = 3001;

const web3 = new Web3("http://127.0.0.1:8545"); // Replace with your Ethereum node URL
const privateKey = "0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266"; // Replace with your private key

const abi = contractAbi.abi;
const contractAddress = "0xe7f1725E7734CE288F8367e1Bb143E90bb3F0512"; // Replace with your contract address
const storage = new web3.eth.Contract(abi, contractAddress);


const sha1 = require("sha1");
const fs = require("fs-extra");
```

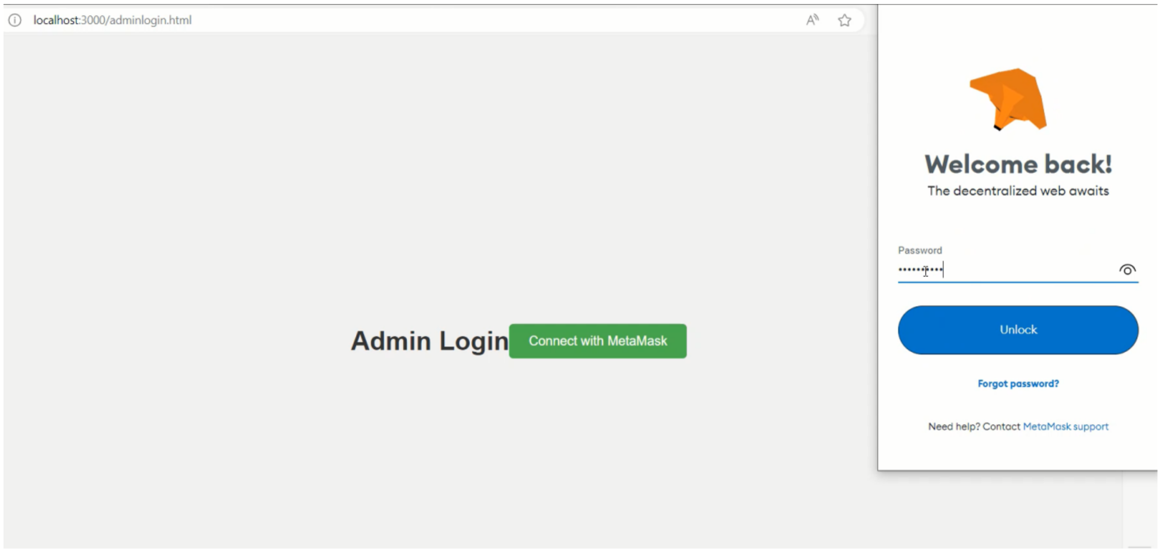
```
PS D:\health\Blockchain-Project\Integration> node server.js

Server is running on http://localhost:3000
```

```
PS D:\health\Blockchain-Project\Integration> node doctor-sc
reen.js
Server is running on http://localhost:3001
```

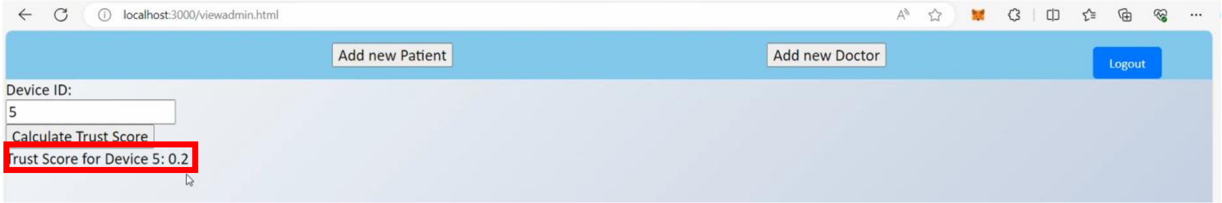
A front end is designed for the use of clients, which is accessible on local host 3000. So http://localhost:3000will open the client web application



When user login it will be authenticated through metamask


localhost:3000/adminlogin.html
Admin Login
Connect with MetaMask
Welcome back!
The decentralized web awaits
Password
Unlock
Forgot password?
Need help? Contact MetaMask support

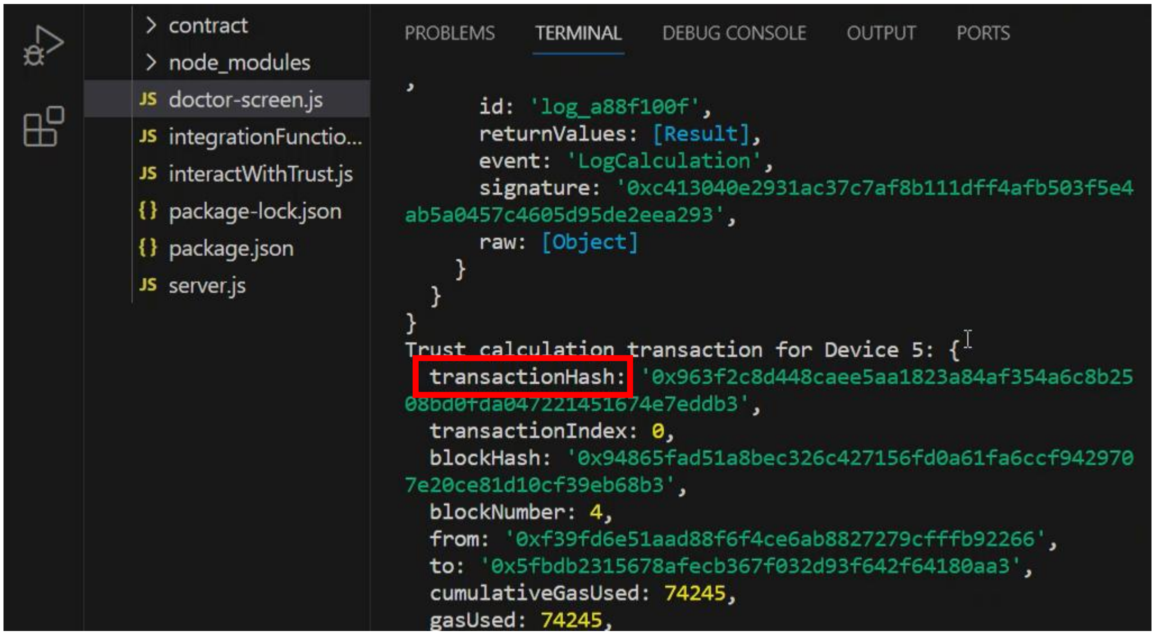
Now admin, after login when enter device ID can view the trust score



Device ID:
5

Trust Score for Device 5: 0.2

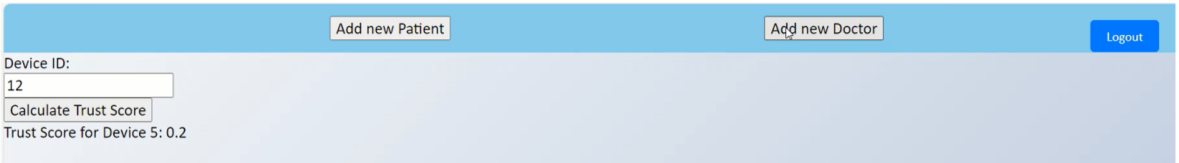
Let’s see the transactions on block chain



```
,
      id: 'log_a88f100f',
      returnValues: [Result],
      event: 'LogCalculation',
      signature: '0xc413040e2931ac37c7af8b111dff4afb503f5e4
ab5a0457c4605d95de2eea293',
      raw: [Object]
    }
  }
}
Trust calculation transaction for Device 5: {
  transactionHash: '0x963f2c8d448caee5aa1823a84af354a6c8b25
08bd0fda047221451674e7eddb3',
  transactionIndex: 0,
  blockHash: '0x94865fad51a8bec326c427156fd0a61fa6ccf942970
7e20ce81d10cf39eb68b3',
  blockNumber: 4,
  from: '0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266',
  to: '0x5fbdb2315678afecb367f032d93f642f64180aa3',
  cumulativeGasUsed: 74245,
  gasUsed: 74245,
```

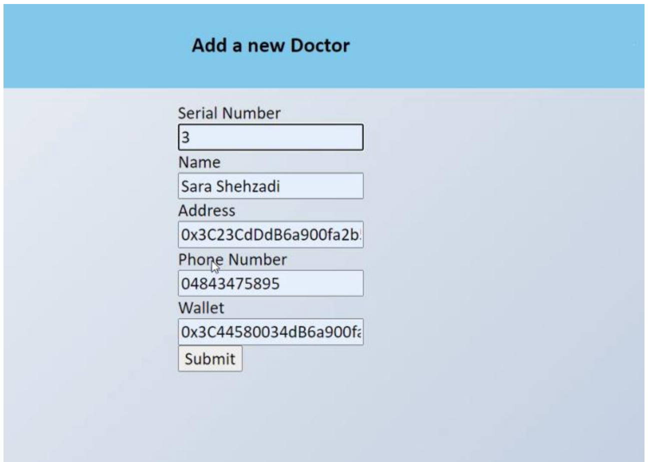
The transaction hash,block hash and block number are highlighted in red.

Now admin will use the function Add Doctor to add a doctor on ACL contract



Device ID:
12

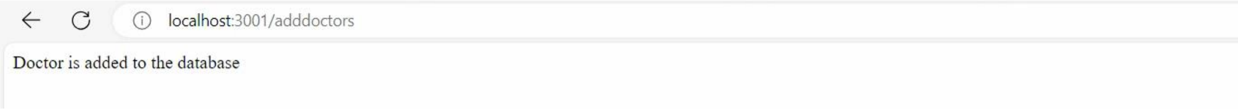
Trust Score for Device 5: 0.2



Add a new Doctor

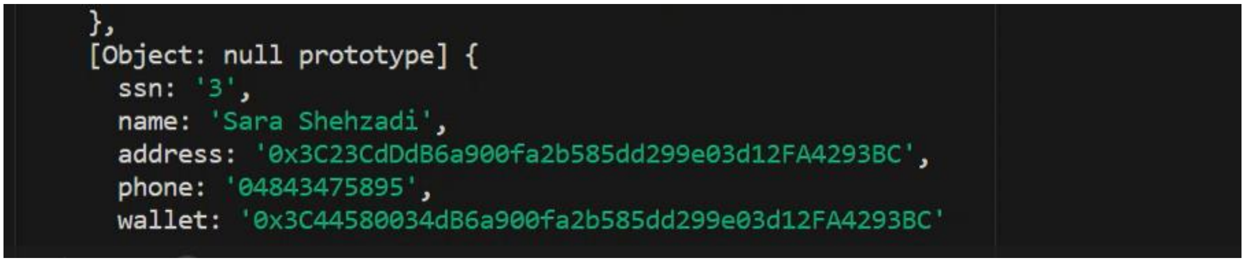
Serial Number
3
Name
Sara Shehzadi
Address
0x3C23CdDdB6a900fa2b
Phone Number
04843475895
Wallet
0x3C44580034dB6a900f

When the admin after filling necessary input fields will submit a successful addition in block chain will show as



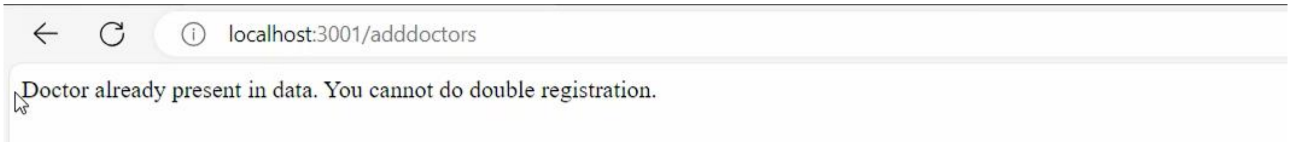
Doctor is added to the database

Same addition can be seen, stored on blockchain



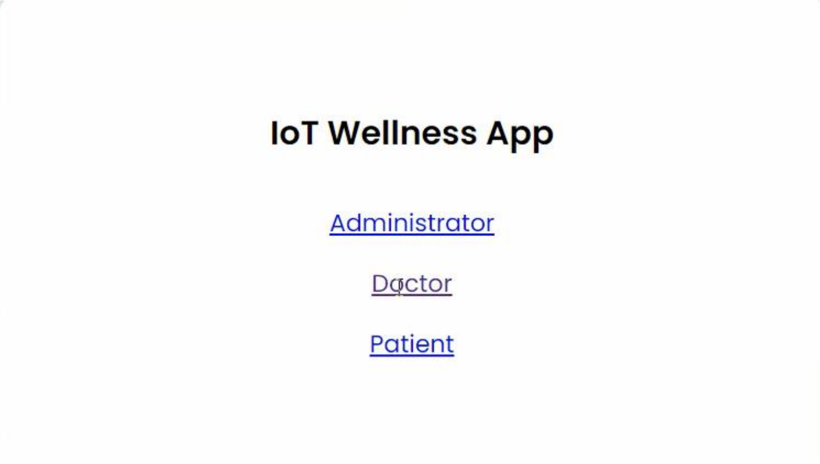
```
    },
    [Object: null prototype] {
      ssn: '3',
      name: 'Sara Shehzadi',
      address: '0x3C23CdDdB6a900fa2b585dd299e03d12FA4293BC',
      phone: '04843475895',
      wallet: '0x3C44580034dB6a900fa2b585dd299e03d12FA4293BC'
```

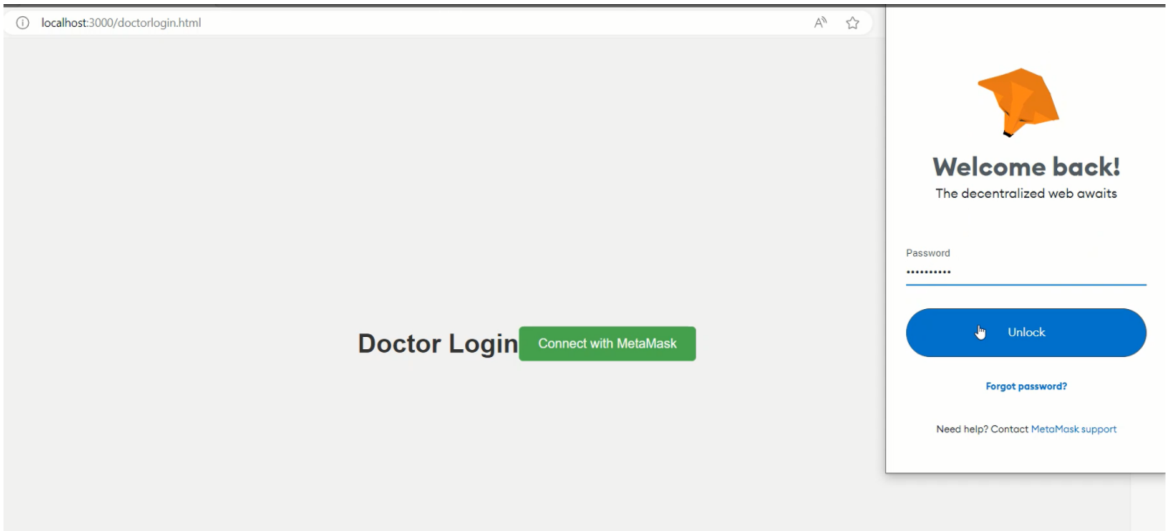
User ID management: A duplicate entry of a registered user is not allowed and the alert will also send to backend that there is some change in values.If again the same entry is submitted it will give an error as



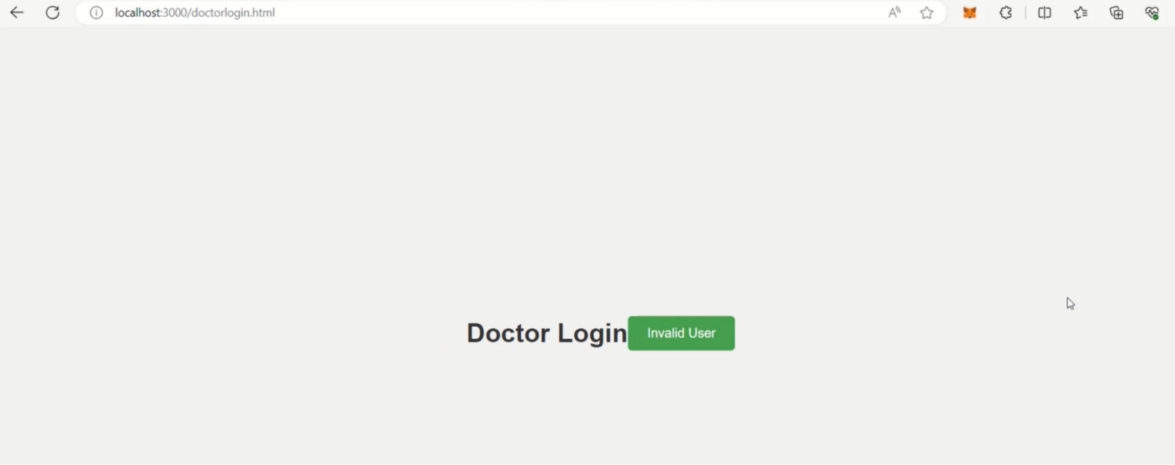
Doctor already present in data. You cannot do double registration.

Then we login as doctor

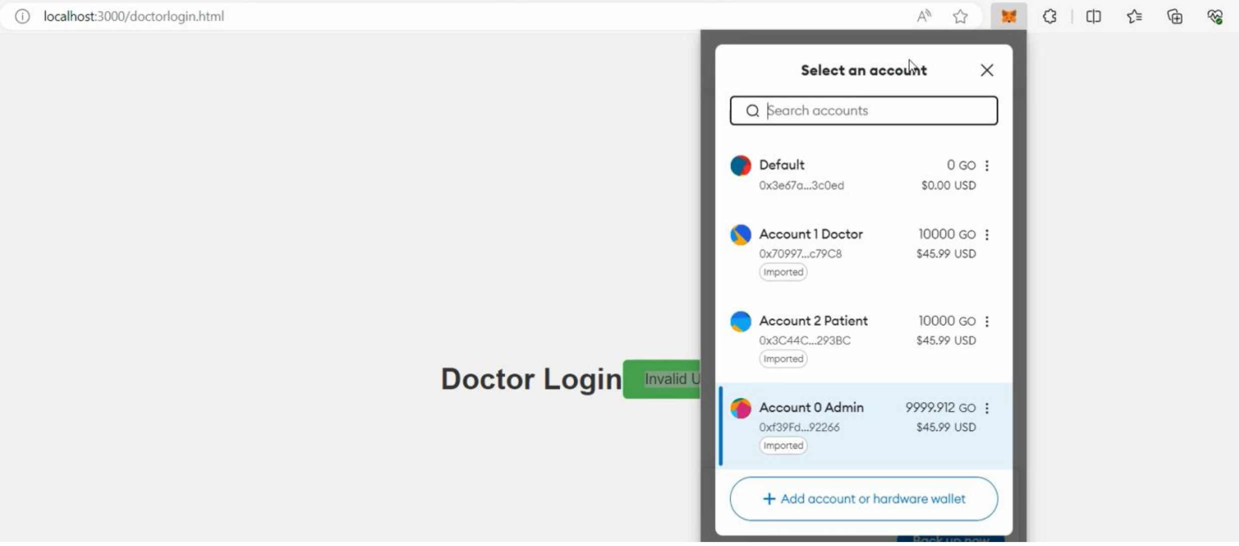



localhost:3000/doctorlogin.html
Doctor Login
Connect with MetaMask
Welcome back!
The decentralized web awaits
Password
••••••••••
Unlock
Forgot password?
Need help? Contact MetaMask support

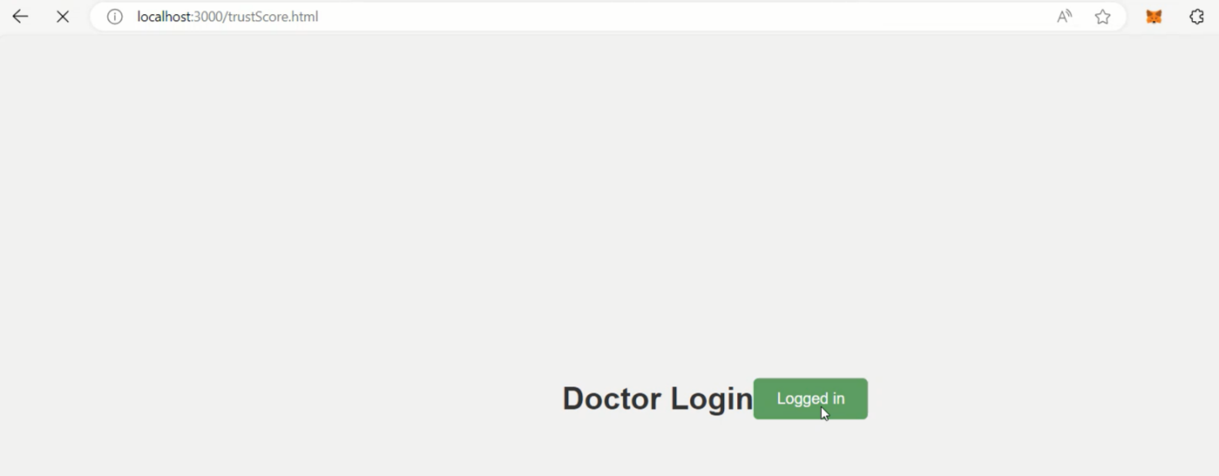
It can be easily seen that when metamask account was on admin ethereum address and it tries to login on doctors page it will give invalid user

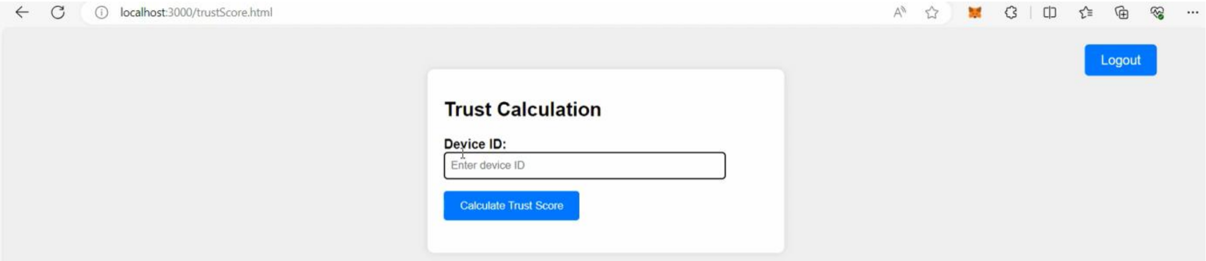


Now let us change the account from admin to doctor on metamask

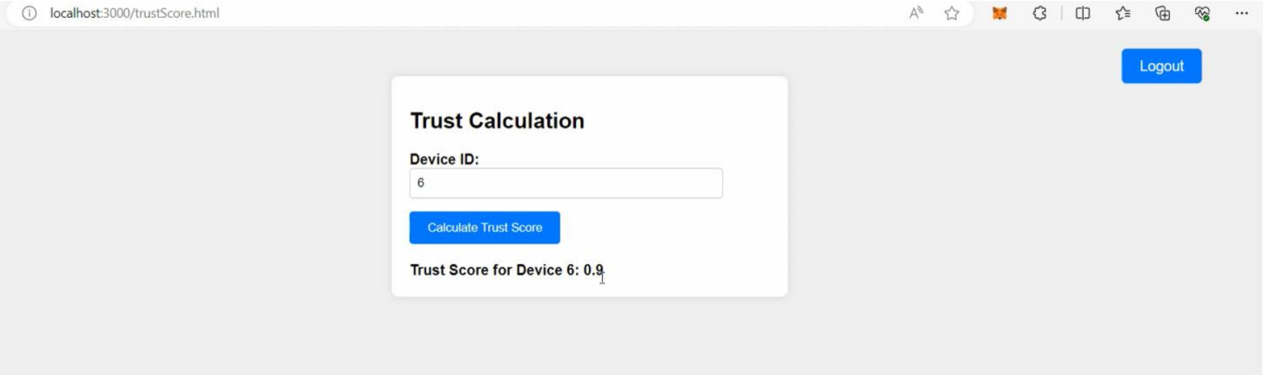

localhost:3000/doctorlogin.html
Doctor Login
Invalid U
Select an account
Search accounts
Default 0 GO
0x3e67a...3c0ed $0.00 USD
Account 1 Doctor 10000 GO
0x70997...c79C8 $45.99 USD
Imported
Account 2 Patient 10000 GO
0x3C44C...293BC $45.99 USD
Imported
Account 0 Admin 9999.912 GO
0xf39Fd...92266 $45.99 USD
Imported
+ Add account or hardware wallet

And then it logins



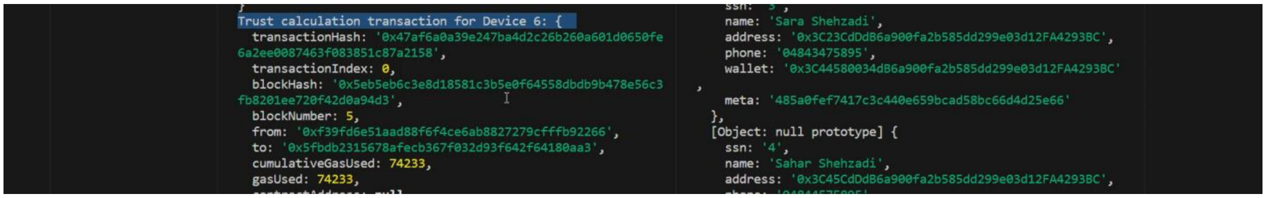


Now when doctor enters device ID it gets trust score



Device ID: 6

Trust Score for Device 6: 0.9

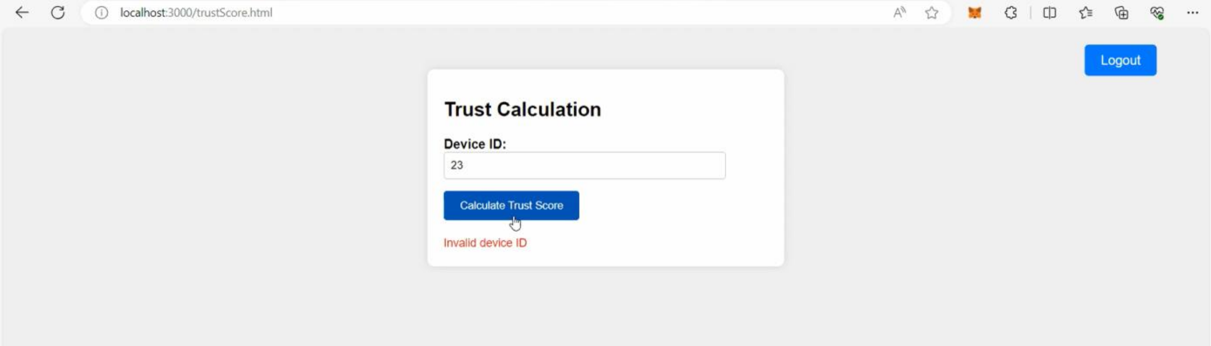


```
Trust calculation transaction for Device 6: {
  transactionHash: '0x47af6a0a39e247ba4d2c26b260a601d0650fe
6a2ee0087463f083851c87a2158',
  transactionIndex: 0,
  blockHash: '0x5eb5eb6c3e8d18581c3b5e0f64558dbdb9b478e56c3
fb8201ee720f42d0a94d3',
  blockNumber: 5,
  from: '0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266',
  to: '0x5fbdb2315678afecb367f032d93f642f64180aa3',
  cumulativeGasUsed: 74233,
  gasUsed: 74233,
```

```
    name: 'Sara Shehzadi',
    address: '0x3C23CdDdB6a900fa2b585dd299e03d12FA4293BC',
    phone: '04843475895',
    wallet: '0x3C44580034dB6a900fa2b585dd299e03d12FA4293BC'
,
    meta: '485a0fef7417c3c440e659bcad58bc66d4d25e66'
  },
  [Object: null prototype] {
    ssn: '4',
    name: 'Sahar Shehzadi',
    address: '0x3C45CdDdB6a900fa2b585dd299e03d12FA4293BC',
```

So this shows that transactions which are done are constantly stored in backend.

It is to be noted that in this prototype we have calculated trust score of 10 devices if user enter wrong device ID it gives an alert



Device ID: 23

Invalid device ID

Same procedure will be followed when patient logins

5.4 Workflow

Fig 5.2 and 5.3 shows the overall workflow

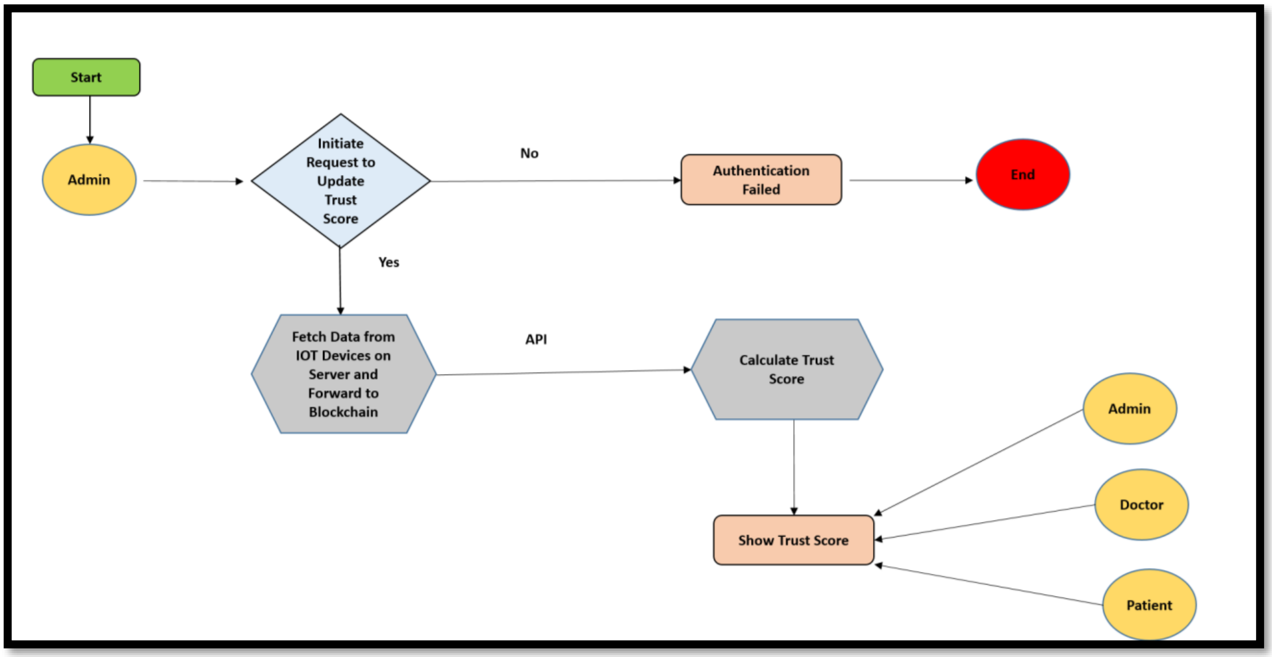

Start
Admin
Initiate Request to Update Trust Score
No
Authentication Failed
End
Yes
Fetch Data from IOT Devices on Server and Forward to Blockchain
API
Calculate Trust Score
Admin
Doctor
Show Trust Score
Patient

Figure 5.2Overall Workflow

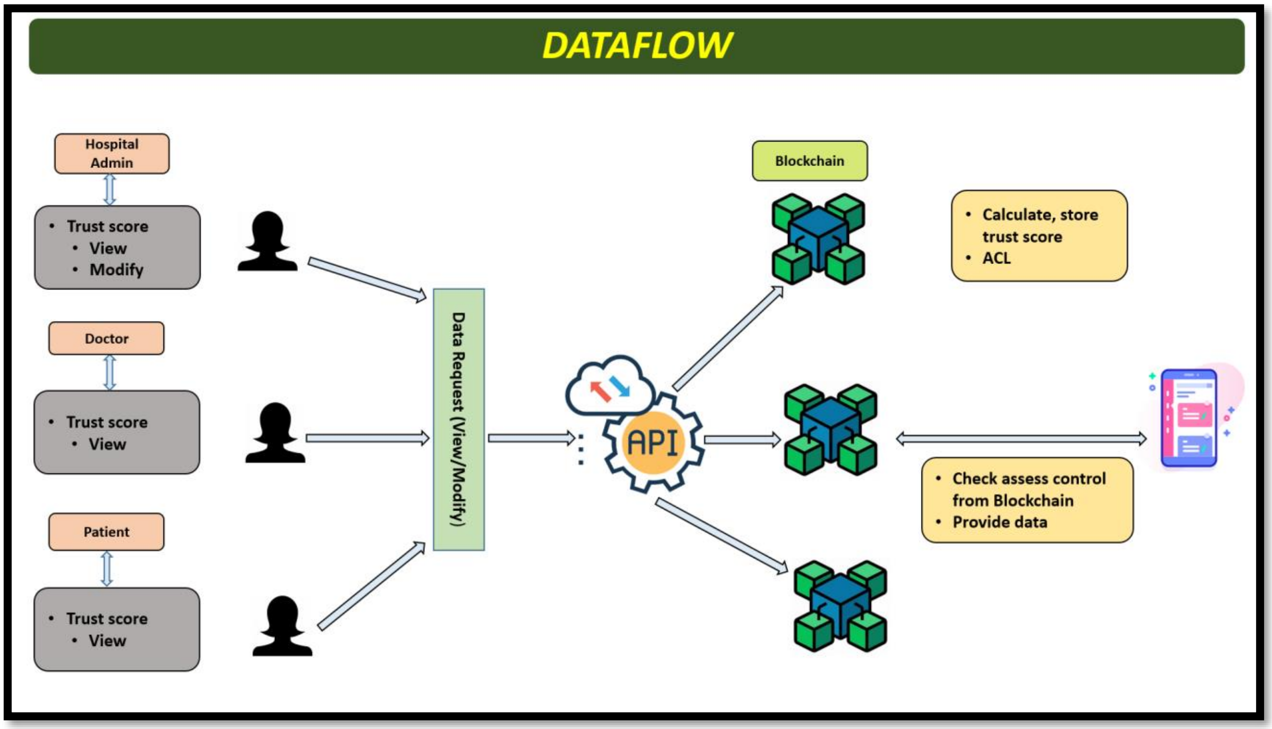


Figure5.3 Diagrammatic view of Dataflow

5.5 Security Analysis:

Table 5 shows how these security objectives are achieved

Security and Privacy Objectives	Configuration
Data Integrity	Data Integrity ,Trust of each device is calculated and stored on blockchain
Transparency	Trust score calculation and storage is on block chain any change will be logged, which makes trust score transparent
Secure Automation	Tamper –proof system of trust calculation of IoT devices

Table 5: Achievement of Security Objectives

Attacks on IoT devices and their mitigation through this research

No of Transactions

Attacks on IoT Devices	Prevention
Bad-mouthing	Trust of different interacting nodes is taken as transaction and transactions are recorded in blocks that are linked together using cryptographic hashes. Once a transaction is recorded and confirmed, it becomes extremely difficult to alter or remove it. This immutability ensures that false information cannot be inserted
On-off attack	If trust value of a node falls below 0.5 for consecutive 5 times, it is banned and discarded from the network. This way no node is unfairly discarded, and we can prevent badmouthing and ballot stuffing attacks
Self-promoting attack	self-promoting node attack, malicious nodes may manipulate their presence and availability in the network, leading to disruptions in communication or false reports of device status

Table 6: Attacks on IoT and their prevention

Chapter 6

CONCLUSION AND FUTURE WORK

6.1. Conclusion

The culminating chapters of this thesis present a robust Blockchain-based trust management framework meticulously designed to cater specifically to the intricate dynamics of Internet of Things (IoT) devices. The core focus of this framework revolves around ensuring the integrity of data, a fundamental aspect crucial for the reliability and functionality of IoT ecosystems. Through a systematic and comprehensive approach, this research significantly contributes to the evolving landscape of trust models in both IoT and blockchain trust management systems.

At the heart of this work lies the groundbreaking development of a context-aware trust model, seamlessly implemented as a smart contract within the blockchain infrastructure. This innovative model goes beyond conventional trust mechanisms by adapting to the contextual nuances of IoT environments. By embedding intelligence into the trust model, the framework is capable of providing nuanced and adaptive trust assessments based on the specific requirements and conditions of the IoT ecosystem.

The integration of this context-aware trust model into the blockchain architecture is a pivotal aspect of this research. Blockchain, with its decentralized and immutable ledger, offers a unique platform for transparent and tamper-proof record-keeping. The trust assessments, carried out through smart contracts, are recorded on the blockchain, providing an auditable trail of trust interactions. This not only enhances transparency but also ensures the reliability of the trust management system.

The significance of this research extends beyond theoretical advancements, as it addresses a critical need in contemporary IoT landscapes. Trustworthy interactions among IoT devices are paramount for the seamless operation of various applications, ranging from healthcare to smart cities. The proposed framework, by laying the foundation for reliable and transparent trust assessments, directly contributes to meeting this demand.

One of the key takeaways from this thesis is the tangible prototype of the proposed framework.

By presenting a practical implementation, the research not only validates the theoretical underpinnings but also offers valuable insights for practitioners and researchers alike. The prototype serves as a proof of concept, demonstrating the feasibility and effectiveness of the context-aware trust model within a blockchain-based environment.

Looking forward, this work sets the stage for future advancements in the realm of blockchain-based trust management. The adaptability of the context-aware trust model opens avenues for further research into refining and extending the framework to address evolving challenges in the dynamic landscape of IoT applications. As the IoT ecosystem continues to expand and diversify, the proposed framework stands as a resilient and forward-looking solution to the ever-growing demand for trustworthy and secure interactions among IoT devices.

In conclusion, this thesis represents a significant contribution to the field of IoT security and trust management. The innovative context-aware trust model, seamlessly integrated into a blockchain framework, not only advances our theoretical understanding but also provides a practical and tangible solution to enhance data integrity and foster trust in the intricate web of IoT applications.

6.2. Future Work

In charting the course for future work, this thesis suggests several avenues that hold promise for expanding and refining the developed Blockchain-based trust management framework tailored for IoT devices. A critical area for exploration is the scalability and performance optimization of the framework, especially concerning the growing number of IoT devices in expansive deployments. Additionally, there is room for research into privacy-preserving trust models, integrating techniques such as homomorphic encryption to ensure trust assessments while safeguarding sensitive information. Further enhancement of the context-aware trust model's adaptability can be pursued through the incorporation of machine learning algorithms that dynamically adjust parameters based on evolving patterns within the IoT environment. Investigating standards for interoperability between different blockchain-based trust management systems and bolstering resilience against advanced attacks are also pertinent areas for future research. Exploring the framework's usability, conducting real-world deployments in diverse IoT applications, and addressing regulatory and ethical considerations are vital steps toward practical implementation. Moreover, the integration of the framework with edge and fog computing, collaborative research with industry partners, and ongoing assessment of its applicability in varied scenarios represent key directions for future exploration, ensuring the continual evolution and effectiveness of blockchain-based trust management systems for IoT security.

References

- Zhang, K., Liang, Z., Huang, X., & Luo, J. (2022). A Blockchain-Based Trust Management Framework for e-Healthcare Systems. IEEE Transactions on Computational Social Systems, 9(1), 196-208.
- Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review
- Blockchain's adoption in IoT: The challenges, and a way forward.
- Trust Chain: Trust Management in Block chain and IoT supported Supply Chains.
- Data Trust framework using blockchain technology and adaptive transaction validation
- Early Access context based adaptive fog computing trust solution for time critical smart health care systems.
- Evaluating critical security issues of the IoT world: Present and future challenges.
- Strengthening the Blockchain based Internet of value with trust Decentralized 2015.
- Sun, Q., Wang, C., & Li, X. (2022). A Blockchain-Based Trustworthy Data Sharing Framework for e-Healthcare Systems. IEEE Transactions on Emerging Topics in Computing, 10(2), 300-312.
- Wang, L., Wang, Y., & Li, Z. (2022). A Blockchain-Based Trust Mechanism for e-Healthcare Systems. IEEE Access, 10, 20767-20780.
- Liu, S., Chen, Y., & Zhou, L. (2021). Blockchain-Based Trust Mechanism for Secure and Efficient Medical Data Sharing. IEEE Access, 9, 48578-48588.
- Xu, Y., Wang, Q., & Zhang, X. (2021). Blockchain-Based Trust Management System for Privacy-Preserving Data Sharing in e-Healthcare Systems. IEEE Transactions on Emerging Topics in Computing, 9(2), 504-514.
- Li, X., & Zhang, X. (2021). Blockchain-Based Trust Model for e-Healthcare Systems Using Fuzzy Logic. IEEE Access, 9, 71017-71030.
- Huang, J., Liu, Y., & Zhang, Y. (2021). Blockchain-Based Trust Management Framework for Secure Data Sharing in e-Healthcare Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(10), 7327-7340.
- Marche and M. Nitti, "Trust-related attacks and their detection: A trust management model for the social iot," IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3297–

3308, 2020.