LEVERAGING CRYPTOGRAPHIC PRIMITIVES OF BLOCKCHAIN FOR TRUST IN SMART SYSTEMS

By

Hafiz Asif Khalil

NUST-2021-MCS-00000397985

Supervisor

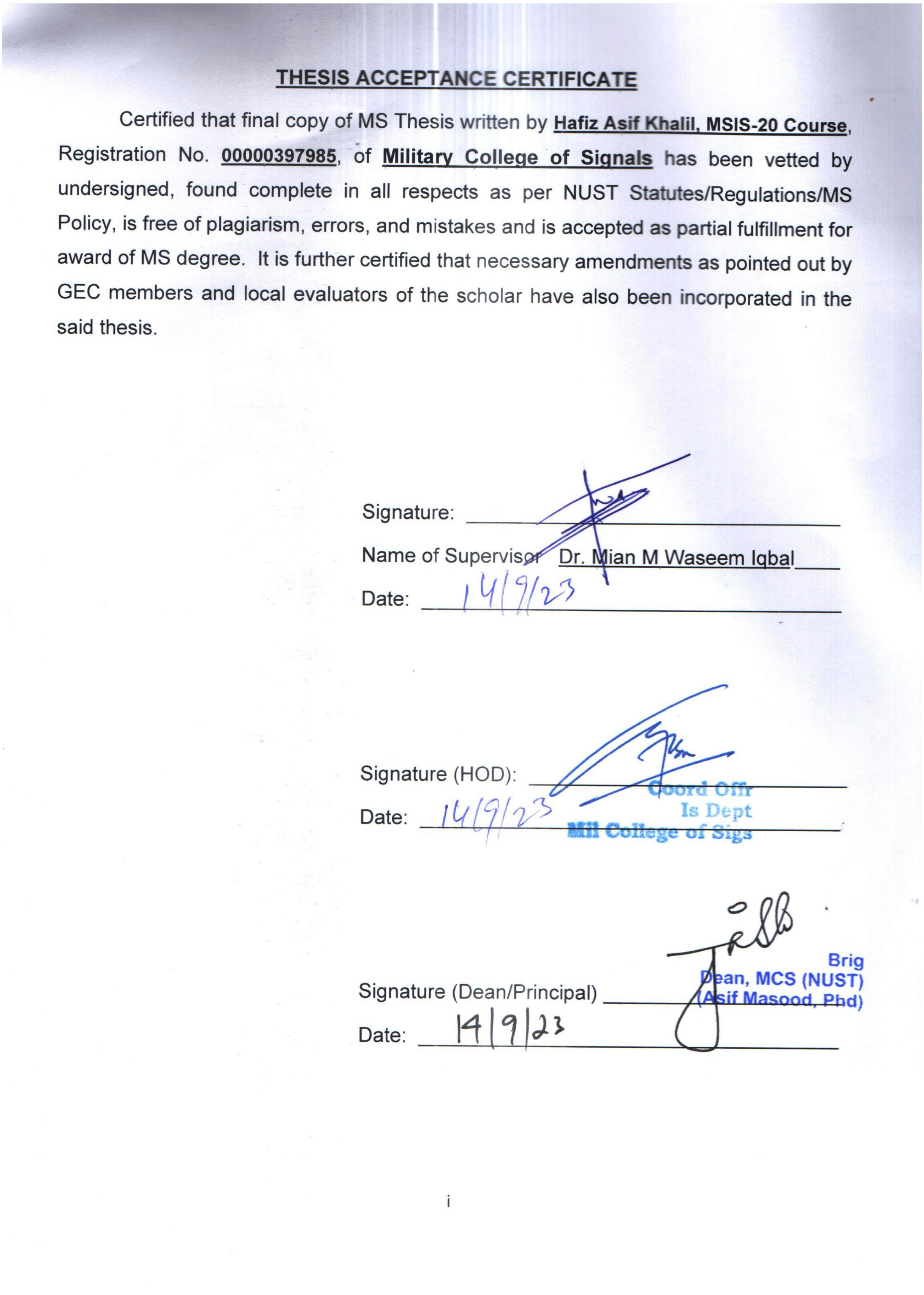
Department of Information Security

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Security (MSIS)

In

Military College of Signals (MCS) ,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(September 2023)



THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Hafiz Asif Khalil, MSIS-20 Course**, Registration No. **00000397985**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: ____________________

Name of Supervisor Dr. Mian M Waseem Iqbal

Date: 14/9/23

Signature (HOD): ____________________

Coord Offr
Is Dept
Mil College of Sigs

Date: 14/9/23

Signature (Dean/Principal) ____________________

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

Date: 14/9/23

Declaration

I hereby declare that no portion of the work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Dedication

To my parents, whose love, encouragement, and sacrifices have made all my achievements possible. Your unwavering belief in me has been a constant source of inspiration. This thesis is dedicated to my brothers and sister who have been my guiding lights and unwavering support throughout my academic pursuit.

To my dear wife and children, for their understanding, patience, and unending encouragement. Their love and support have been my rock during the challenging times of this journey.

To my mentor and advisor, Dr.Mian Muhammad Waseem Iqbal, for their wisdom, guidance, and faith in my abilities. His mentor-ship has shaped me into a better researcher.

To my friends, who have been my pillars of strength and a source of joy throughout this academic endeavor. Your camaraderie has made this journey memorable.

Acknowledgement

First and foremost I am very grateful to ALMIGHTY ALLAH, The most gracious and the most merciful, who bestowed upon me health, wisdom, knowledge, and the power of communication. I owe a great deal to my supervisor for valuable guidance, encouragement, and supervision, which made it possible for me to undertake this project and complete my training in this area. I am deeply obliged for the support of my colleagues especially, Syed Munir Hussain Shah, Haseeb Ahmad, Muhammad Iqbal, Qasim Ali, Ammar Hassan, Huzaifa Ali and Talha Ali whose cooperation proved very helpful in the compilation of my thesis. I am also gratified to put words of thanks to my parents, my wife, and my kids for their motivation, sacrifice, cooperation, love, and affection helping me tide over my difficulties and enable me to complete this research work.

Abstract

Smart systems are very common nowadays like smart cities, smart vehicle parking systems, smart buildings, etc. Any smart system is smart only till the time, all components of it are exchanging data among each other without any fear of data theft and modification. There are several issues and challenges with current smart systems, Many existing smart systems rely on centralized trust authorities, which can be vulnerable to attacks, single points of failure, and compromised trust. Current systems often struggle with maintaining user privacy while establishing trust. Moreover, Ensuring the integrity and authenticity of data is crucial in current smart systems. Nodes in a smart system, do calculate the trust of every other related node depending upon their experience with that specific node and recommendations of other nodes about that specific node. Trust once calculated is prone to integrity attacks by malicious nodes in the system.

Bad-mouthing and ballot stuffing are two common attacks that affect the complete trust calculation mechanism and the final trust values. To avoid such attacks, trust can be calculated by blockchain and once calculated, It can be stored on the chain so that it can be retrieved whenever needed by any desirous node avoiding integrity issues and mitigating many threats.

Hyper Ledger Fabric is a private, permissioned blockchain and can be used by smart devices for calculations and storage of trust values of each node in a decentralized manner. This research focuses on securing the trust calculation mechanism using a private instance of Hyper ledger Fabric. We implemented a healthcare scenario on an HLF network and simulated the secure trust calculation of trust among IoT devices on the chain. The results prove that by using the cryptographic properties of Blockchains, we can improve the overall security and trust in an IoT system.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

In recent years, the convergence of advanced technologies has ushered in a new era of interconnectedness and intelligence, giving rise to a paradigm known as "smart systems." These systems, which encompass various domains such as healthcare, supply chain, energy, and transportation, leverage the capabilities of the Internet of Things (IoT), artificial intelligence, and distributed computing to enable seamless interactions, automation, and data-driven decision-making. However, the widespread adoption of smart systems presents a host of challenges, with one of the most crucial being the establishment and preservation of trust in an inherently decentralized and complex environment.

Every smart system has to face a lot of challenges. IoT devices are the weak link in it. A number of digital devices of any make and type, connected through the Internet are called the Internet of Things. A lot of sensors and processing devices part of a smart system, are exchanging thousands of Giga of data on a daily basis. Without real-time communication of IoT devices, no smart system can work. IoT devices having different origins have multiple constraints i.e. low storage, low power, battery operation, and security/privacy issues. Being versatile in nature, IoT devices are part of different smart systems like Smart Cities, Smart industries and smart buildings, etc. While exchanging data between different nodes of a smart system, security issues are very important. Authentication of legitimate users along with confidentiality, integrity, and privacy of data is of prime importance.

1.2 Limitations of IoT Devices

IoT Devices part of a smart system have many limitations. Due to their limitations, they are of great concern for every researcher and problem solver. A few of the limitations of IoT devices are as under:-

1.2.1 Data storage and Manipulation

IoT devices and sensors in any smart system have limited storage and processing power to manipulate the data. Internet of Things (IoT) devices often have limited memory resources due to their small form factors, energy constraints, and cost considerations. These limitations can impact the functionality and capabilities of IoT devices.

1.2.2 Latency

The processes are time sensitive and require minimum time delays. Some applications, such as real-time control systems or remote surgeries, require low latency. However, the delay introduced by network communication in IoT setups can be problematic for such use cases.

1.2.3 Security and Privacy

Securing data and maintaining data integrity and privacy is of utmost importance as these affect business processes. Malicious nodes can spoil the trust of service providers in smart systems. Trust among different identities of a smart system is necessary for smooth running and safety and security of the smart system. IoT devices often lack robust security features, making them vulnerable to hacking and unauthorized access. This can lead to data breaches, privacy violations, and even the compromise of critical systems.

1.2.4 Firmware Updates and Support

Ensuring that IoT devices receive timely firmware updates for security and functionality improvements can be a challenge, especially for devices with limited resources or those that are no longer actively supported by manufacturers.

1.2.5 Data Management

IoT devices generate vast amounts of data, which can be difficult to manage, process, and analyze effectively. Storing and processing this data efficiently can require significant resources.

1.2.6 Power Consumption

Many IoT devices are battery-powered, which can limit their functionality and lifespan. Optimizing power consumption while maintaining necessary features can be challenging.

1.2.7 Reliability

IoT devices heavily depend on network connectivity and can be rendered useless or unreliable if the network goes down or experiences disruptions.

1.2.8 Scalability

As the number of IoT devices grows, managing and scaling these devices can become complex and resource-intensive. Network congestion and data overload can also be issues.

1.2.9 Interoperability

Different IoT devices are often produced by different manufacturers, using various communication protocols and standards. This can create challenges in getting devices from different vendors to work together seamlessly.

1.2.10 Cost

Developing and deploying IoT devices can be expensive, especially when considering factors like hardware, software, maintenance, and connectivity.

1.2.11 Reliability and Durability

IoT devices deployed in harsh environments, such as industrial settings or outdoor locations, may face challenges in terms of durability and reliability under extreme conditions. Table number 1.1 summarizes the limitations of IoT devices with suggested remedies.

Table 1.1: Limitations of IoT devices and their suggested mitigation

Ser No	***Limitation***	***Category***	***Description***	***Mitigation Techniques***
1	Data storage and Manipulation	Technical Limitation	IoT devices often have limited storage capacity and processing capabilities, which can impact their ability to store and process data efficiently.	Use data compression techniques, offload processing to the cloud, and implement data aggregation strategies.
2	Latency	Technical Limitation	The delay in data transmission and processing can lead to latency issues in real-time applications, affecting responsiveness and user experience.	Optimize communication protocols, use edge computing, and minimize data transmission distances.
3	Security and Privacy	Security Concern	IoT devices are susceptible to security breaches and data privacy concerns due to weak security measures and potential vulnerabilities.	Implement strong encryption, regular security audits, user authentication, and authorization mechanisms.

Continued on next page

Table 1.1 – *Continued from previous page*

Ser No	***Limitation***	***Category***	***Description***	***Mitigation Techniques***
4	Firmware Updates and Support	Technical Limitation	Ensuring that IoT devices receive regular updates and ongoing technical support can be challenging, leading to potential vulnerabilities and obsolescence.	Implement Over-The-Air (OTA) updates, provide long-term support commitments, and manage device life-cycle.
5	Data Management	Technical Limitation	Managing and analyzing the massive amounts of data generated by IoT devices can be complex, requiring efficient data management strategies.	Use data analytics tools, data filtering, edge analytics, and efficient data storage solutions.
6	Power Consumption	Technical Limitation	Many IoT devices operate on batteries or low power sources, leading to concerns about power efficiency and the need for frequent recharging or replacement.	Optimize power usage, implement energy harvesting, low-power communication protocols, and sleep modes.

Continued on next page

Table 1.1 – *Continued from previous page*

Ser No	***Limitation***	***Category***	***Description***	***Mitigation Techniques***
7	Reliability	Technical Limitation	Ensuring consistent and reliable operation of IoT devices is crucial, especially in critical applications, to avoid failures and disruptions.	Implement redundancy, fail over mechanisms, continuous monitoring, and predictive maintenance.
8	Scalability	Technical Limitation	As IoT ecosystems grow, managing and scaling the infrastructure can become complex, requiring careful planning and management.	Use cloud computing, modular architecture, horizontal scaling, and load balancing techniques.
9	Interoperability	Technical Limitation	Lack of standardized protocols and compatibility can hinder seamless communication and integration between different IoT devices.	Adopt industry standards, use open protocols, promote interoperability testing, and develop APIs.
10	Cost	Economic Limitation	The cost of developing, manufacturing, and deploying IoT devices can impact their accessibility and adoption in various contexts.	Optimize design for cost efficiency, explore economies of scale, consider long-term costs.

Continued on next page

Table 1.1 – *Continued from previous page*

Ser No	*Limitation*	*Category*	*Description*	*Mitigation Techniques*
11	Reliability and Durability	Technical Limitation	IoT devices exposed to various environmental conditions and physical stress need to be durable and reliable over time.	Use ruggedized designs, environmental testing, proper material selection, and protective enclosures.

1.3 Falling Trust

In the wake of the above limitations of IoT Devices, trust in IoT devices of Smart systems is highly suspicious. A compromised IoT device is very harmful to any smart system. A smart system unaware of the compromise of its IoT devices is highly dangerous.
Trust is a cornerstone of any successful system, influencing user behavior, data sharing, and collaboration. Traditional centralized models of trust, where a central authority arbitrates and maintains trust, are often inadequate in the context of smart systems. As these systems operate across distributed networks, the need arises for novel mechanisms that can ensure trust without relying on a single point of control.

1.4 Usage of Blockchain to Enhance Trust

This is where blockchain technology and its cryptographic primitives emerge as transformative tools. [1] Blockchain, a distributed and immutable ledger technology, gained prominence through its pioneering application in cryptocurrencies. However, its potential extends beyond digital currencies, with applications spanning supply chain transparency, digital identity, secure data sharing, and decentralized applications. At the heart of blockchain's functionality are cryptographic primitives that underpin its security, immutability, and consensus mechanisms. [2] In the context of smart systems,

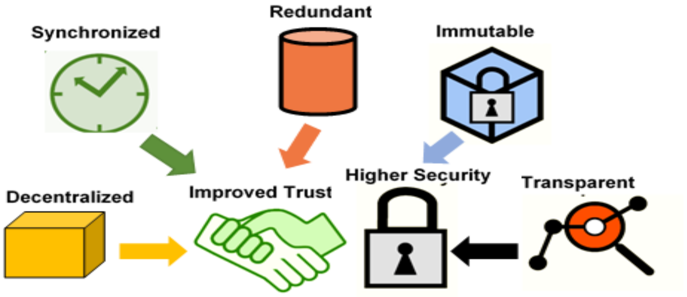


Figure 1.1: Improving Trust with the usage of basic primitives of The Blockchain

where participants interact autonomously and dynamically, trust becomes multifaceted. It encompasses not only the authenticity and integrity of data but also the behavior and intentions of entities within the system. Cryptographic primitives offer a means to establish and validate these facets of trust in a decentralized manner, ensuring that smart systems operate reliably and securely. [3]

This research work explores the potential of leveraging the cryptographic primitives of blockchain technology to enhance trust within smart systems. By employing cryptographic techniques such as digital signatures, and hashing, this research aims to develop robust mechanisms for trust establishment, verification, and management. The goal is to address challenges related to data integrity, authentication, authorization, and privacy within the context of smart systems.

1.5 Scope

The scope of this research work encompasses a comprehensive review of existing cryptographic primitives used in blockchain technology and their applicability to smart systems. Through case study, the research will assess the effectiveness of these primitives in enhancing trust within specific domains of healthcare.

1.6 Problem Statement

In today's increasingly interconnected world of smart systems, which encompass a broad spectrum of applications ranging from IoT (Internet of Things) devices to autonomous vehicles, trust is a fundamental cornerstone for seamless and secure operation. Trust involves not only the assurance of data integrity and authenticity but also the establishment of reliable identities and secure communications among these devices. However, the traditional models of trust that rely on centralized authorities and intermediaries are ill-suited for the decentralized and autonomous nature of smart systems. Furthermore, the ever-growing volume of sensitive data generated and exchanged within these systems intensifies the urgency of finding robust trust solutions.

1.7 Research Objectives

The main objectives of this thesis are:-

- To study the current threats and limitations of IoT devices in any smart system and apply different protocols of blockchain to mitigate the issue.
- To propose an effective Enterprise and private blockchain for calculations and storage of adaptive trust to preserve data integrity in any smart environment of IoT. The proposed solution is expected to improve performance while mitigating threats like the Sybil attack, Bad Mouthing attack, Ballot stuffing attacks, and On Off attack.
- Comparative analysis of the proposed scheme with the existing solutions available.

1.8 Contributions

The research aims to:-

- Provide more effective and foolproof data integrity and logging mechanism.for sensitive data.
- Minimize the occurrence of security breaches to a negligible level.

- Ensure that the stakeholder will be the real owner of its data, he will be authorizing the entity to share its data with anyone.
- Increase stakeholders' confidence in the system.
- provides a framework that can be used for calculation and storage of trust values of different IoT devices.

1.9 Thesis Outline

This Research work aims to contribute to the emerging field of trust in smart systems by exploring the synergies between cryptographic primitives and blockchain technology. By addressing the challenges of trust in decentralized and dynamic environments, this research seeks to pave the way for more secure, reliable, and resilient smart systems that can unlock the full potential of the digital age.The research work has been organized into following chapters:-

- **Chapter 1:** Firstly a brief introduction is mentioned discussing the limitations of IoT Devices and lowering the trust values, followed by the discussion of possibility of usage of blockchain to address the issue. Research objectives are listed and in the end, something about the contribution we intend to make through this research.
- **Chapter 2 :** Provides a detailed background knowledge of Trust, its calculations, and Trust-related Attacks. This chapter also explains the current blockchain architecture being widely used.
- **Chapter 3:** Describes the research work carried out so far for the provision of trust in different smart systems.
- **Chapter 4:** Is about a case study pertaining to the health care system. In this section, the possibility of the usage of blockchain technology for the calculation and preservation of trust values is discussed in length.
- **Chapter 5:** Presents the methodology employed and the proposed solution along with the proposed architecture.

- **Chapter 6:** This chapter presents the analysis and results of the proposed solution and architecture. This chapter also discusses the effectiveness of leveraging cryptographic primitives for trust enhancement.
- **Chapter 7:** This Chapter concludes the paper by summarizing the contributions, discussing the limitations of the study, and proposing avenues for future research.

Chapter 2

Trust Cycle, Related Attacks, and Current Blockchain Architecture

2.1 Trust

Trust is the level of assurance about an identity that it will behave in a certain way under certain circumstances [4] [5]. Trust is indeed a complex concept that involves the belief or confidence that someone or something will act in a reliable, consistent, and predictable manner. It is the assurance that someone or something will behave, perform, or deliver as expected, even when there is uncertainty or vulnerability involved. It is a fundamental aspect of interaction and plays a crucial role in various domains. Trust can be categorized into different phases or dimensions.

2.2 Trust Cycle

Trust calculation is divided into four different phases:-

2.2.1 Information Collection

Combination of direct and indirect observation is used for the collection of information for calculations of trust.

- Direct Observation:- When a user or a node directly interacts with another node or server and calculates the trust depending upon its own experience of that interaction.

- Indirect Observation:- When a user goes for an indirect recommendation from other neighboring nodes about a specific node or server without having direct interaction with a specific node or server, it is termed as Indirect Observation and trust calculated in this way is called Indirect Trust. This type of trust is very important and needs more care.

2.2.2 Selection of trust Model

After the collection of information about a specific node, we have to select a trust model either a decision model or an evaluation model. Decision model can be any of the following three types:-

- History based
- Recommendation based
- Hybrid of both

Few examples of Evaluation models are:-

- Reputation model
- Behaviour Model
- Probabilistic model
- Fuzzy Model
- Simple Statistical Model
- Discrete Mode

2.2.3 Trust Processing

When information is collected and trust model is selected, next step is to decide how we will process the trust. There are two ways of processing the trust.

- Centralized:- In this way of processing, one node is made responsible for calculating the trust for all entities in a system. It avoids the communication overhead between the nodes but poses a single point of failure problem.
- Decentralized:- Each node will calculate trust for itself instead of a central node. This kind of trust processing avoids a single point of failure as it was in the case of centralized processing.

2.2.4 Trust Update

the Last phase of trust calculation is to decide the frequency of trust calculation. At what time and after how much interval trust will be recalculated? Any one approach out of the following three can be adopted.

- Event Driven:- Whenever any incident happens fresh.
- Time Driven:- A time is defined after which fresh trust will be calculated periodically.
- Continuous:- Trust is being updated as a continuous process. Trust is being updated continuously without waiting for any incident or time interval. trust is calculated.

Figure 2.1 depicts a graphical view of the Trust cycle describing all 4 phases of trust.

2.3 Trust Parameters

Trust parameters are required to be selected on which trust is to be calculated. A few of the possible factors can be:-

2.3.1 Latency

Time taken for data to travel from source to destination.

2.3.2 Packet Loss Ratio

Ratio of successfully delivered packets to total packets sent.

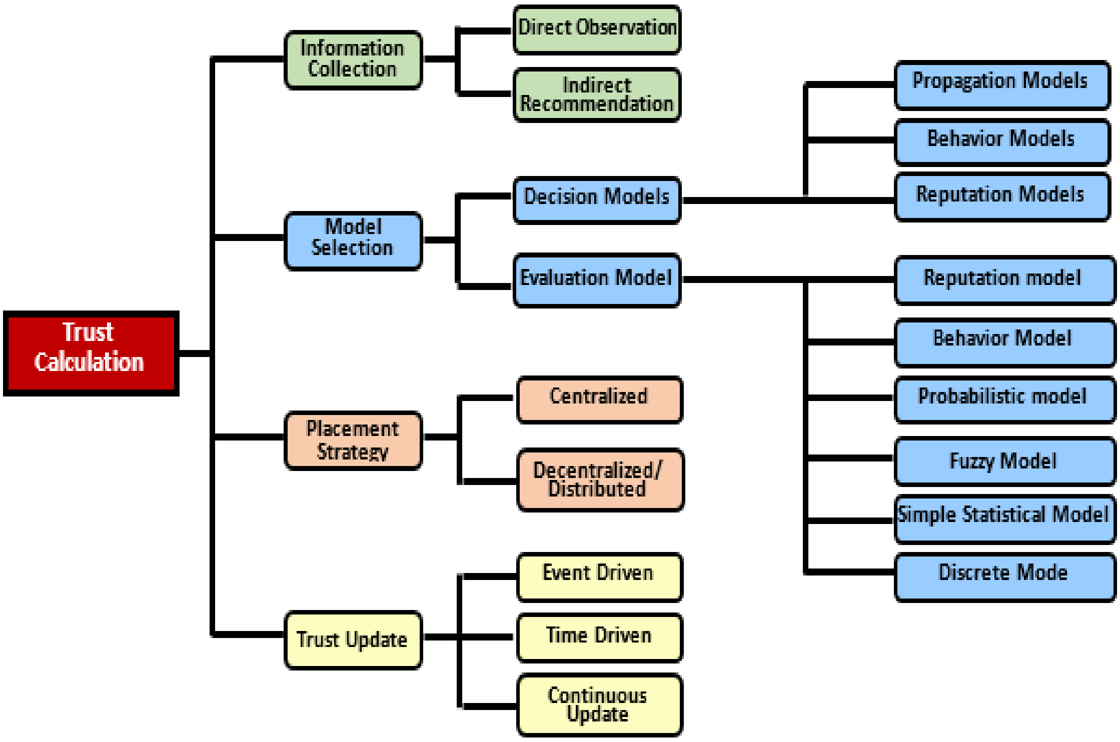


Figure 2.1: Steps involved in calculation of Trust of any interacting device

2.3.3 Throughput

Rate of data transmission

2.3.4 Bandwidth Utilization

Efficient use of available bandwidth.

2.3.5 Response Time

Time taken to send a request and receive its response at the service requester is called response time.

2.3.6 Jitter

The variation in delay between received data packets in a network.

2.3.7 Packet Loss Ratio

The percentage of data packets that are lost during transmission between the IoT device and its intended destination.

2.4 Adaptive or Context-based trust calculation

Trust is not an absolute thing rather it is a relative term. If we consider our daily routine life, if someone has trust in another, it reflects its positive observation and experience about interaction with that specific entity. Trust remains the same as long as the context remains the same. By changing the context trust is changed [6], [7], [8]. For example, if a trustor is having some service from a trustee, the following factors may play a key role in calculating the trust on the trustee.

- Server providing the service
- Location of the server providing services
- Type of service
- List of social contacts of a recommender recommending the trust of a server

Until and unless the above-mentioned factors are the same, trust on a trustee is the same. By changing these factors, context is changed, hence, trust is changed. Context-based or context-aware trust is a step ahead of normal trust. After defining and explaining context-aware trust, how trust is calculated? While there is not a single formula that universally defines trust, you can create a trust score or metric by considering multiple elements and assigning weights to them based on their importance in your specific context. Trust may be calculated in three steps:-

- Direct Trust
- Indirect Trust
- Total Trust

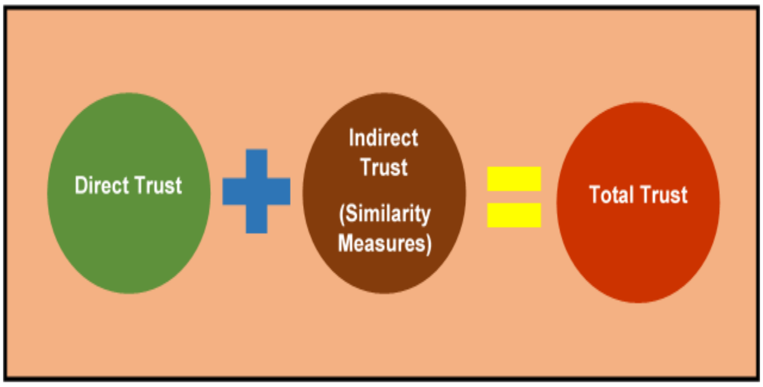


Figure 2.2: Total Trust combination of Direct and Indirect Trusts

2.5 Total Trust

Total trust is calculated by adding direct and indirect trust keeping in view the weight parameter. Figure 2.2 shows how total trust is calculated.

2.5.1 Direct Trust

To calculate the direct trust of the interacting nodes, first of all, we have to decide our trust parameters. We will use latency, packet delivery ratio, and response time to calculate trust. Proper weights are assigned to these parameters. Any node having completed its interaction with another node, will calculate the values of the above trust parameters, and direct trust will be calculated.

2.5.2 Indirect Trust

If a Node has not interacted with another node. Indirect trust will be calculated and it will be calculated from the recommendations of the nodes that have already interacted. It is the point where context-based trust or adaptive trust will play its role. To check whether the context is the same or changed a similarity measure is introduced. This similarity measure will check how much the context of a recommender is the same. Following Similarity checks can be applied.

- Server Similarity
- Server location similarity
- Service similarity

2.6 Trust Related Attacks

Different types of attacks related to trust are as under:-

2.6.1 Bad Mouthing Attack or Misleading feedback Attack

In this type of attack, bad recommendations of an honest node are given to miscalculate the trust about the targeted node. A Bad Mouthing Attack, also known as a Misleading Feedback Attack, is a type of malicious activity that occurs in reputation systems, online reviews, or feedback-based platforms. In this attack, an entity intentionally provides false, negative, or misleading feedback about another entity's reputation or performance to tarnish its image or manipulate the reputation system for personal gain. This type of attack aims to undermine the trust and credibility of the targeted entity within the community or system.

2.6.2 Sybil Attack

A Sybil Attack is a type of malicious activity in computer networks and distributed systems, where a single adversary creates multiple fake identities or nodes to gain a disproportionately large influence or control over the network. In this type of attack, a single node may generate multiple fake IDs, and these IDs are used to give false recommendations about a targeted node. This attack is named after the book "Sybil" by Flora Rheta Schreiber, which documented the case of a woman with dissociative identity disorder who exhibited multiple personalities.

2.6.3 New Comer Attack

In this Attack a node with a bad reputation leaves networks and re-enters the same network with another name and identity thus able to avoid its past misbehavior in the network. This type of attack exploits the decentralized nature of networks and reputation systems, where participants may have limited information about each other's real-world identities. By creating multiple fake identities, the attacker can reset their reputation and evade any negative history associated with their previous identity.

2.6.4 Self-Promoting Attack

A Self-Promoting Attack, also known as a Collusion Attack or Shilling Attack, is a deceptive and manipulative tactic where entities, often acting in coordination, promote themselves or their products/services to gain an unfair advantage within a system, platform, or community. This type of attack aims to artificially boost the reputation, visibility, or popularity of certain entities, leading to skewed outcomes, unfair competition, or misleading perceptions. In this attack, a node is sending good reports about itself to all the nodes for being selected as a service provider.

2.6.5 On-Off Attack

A malicious node behaves as a good node for most of the time but occasionally exhibits malicious behavior for short periods to avoid detection, is commonly known as a "Sleeping-Beauty Attack" or "On-Off Attack." This attack is a form of deception where the malicious node strategically alternates between benign behavior and malicious behavior to evade detection mechanisms. A malicious node may act as a good one for maximum duration and acts as a bad node for a little duration to avoid detection.

2.6.6 Ballot Stuffing Attack

If malicious nodes are given high ratings and their reputation is falsely enhanced, it is called a ballot stuffing attack. A Ballot Stuffing Attack is a form of electoral or voting fraud where an adversary manipulates the voting process by submitting a large number of fraudulent votes or ballots. This attack is named after the practice of "stuffing" additional ballots into a ballot box to skew the results in favor of a particular candidate or outcome. Ballot stuffing attacks can occur in both physical voting systems and online/virtual voting platforms.

2.6.7 Injecting Fraudulent Packets

In this attack, new fraudulent packets are injected into the ongoing communication path. Packets can be replayed and their integrity can also be changed. Injecting Fraudulent Packets is also known as Packet Injection attacks. It is a cyber-attack where an adversary sends unauthorized or falsified network packets into a communication network. This attack aims to disrupt communication, compromise network security, or manipulate network behavior by introducing malicious packets that mimic legitimate traffic.

2.6.8 Selective forwarding attack

A Selective Forwarding Attack is a type of cyber attack that targets communication networks, particularly in wireless sensor networks and other distributed systems. In this attack, an adversary selectively chooses to forward or drop specific packets within the network, leading to a disruption in communication and potentially affecting the network's overall performance and functionality.

2.6.9 Black Hole Attack

When all the packets are dropped and no packet is able to reach the concerned node, it is called black hole attack. A Black Hole Attack is a type of cyber attack that targets communication networks, particularly in wireless networks and mobile networks. In this attack, a malicious node within the network behaves as a "black hole" by falsely advertising itself as having the shortest route to a destination node. As a result, legitimate data packets are routed to the malicious node, which drops or consumes them, effectively disrupting communication.

2.6.10 Sink Hole Attack

In this attack, the malicious node pretends to be the shortest node in the path of packets and attracts all the packets at the shortest distance. A Sinkhole Attack is a type of cyber attack that targets communication networks, particularly in wireless networks and sensor networks. In this attack, a malicious node or attacker manipulates the network's routing process to attract and redirect traffic, effectively creating a "sinkhole" where data converges and is trapped. Sinkhole attacks can disrupt communication, compromise network security, and enable the attacker to intercept or manipulate the trapped data.

2.6.11 Warm Hole Attack

2x malicious nodes create a tunnel among each other and attract all the packets of a network to route through this tunnel. In this attack, malicious nodes create a "wormhole" by capturing packets at one location in the network and then tunneling and replaying them at another location. This can lead to a variety of security and communication issues, including disruption of routing, information interception, and data manipulation.

2.6.12 Grey Hole Attack

Accepting few packets and dropping the few packets is called the Grey Hole Attack. A Grey Hole Attack, also known as a Partial Denial of Service (DoS) Attack, is a type of cyber attack that targets communication networks. In a Grey Hole Attack, a malicious node selectively drops or delays a portion of the network's traffic while allowing other traffic to pass through normally. This attack aims to disrupt communication without completely blocking it, making it difficult to detect malicious behavior.

2.6.13 Flooding Attack

In this Attack, a Malicious node sends so many packets in the communication path that are beyond the handling capacity of the system. A Flooding Attack, also known as a Network Flooding Attack or Packet Flooding Attack, is a type of cyber attack where a large volume of malicious traffic is intentionally sent to a target network or system with the aim of overwhelming its resources and causing disruption or denial of service. This attack is designed to exhaust network bandwidth, processing power, or other resources, rendering the targeted system slow or completely unavailable.

2.6.14 Discrimination Attack

If a service is being provided from a server, good service will be provided to a group and bad service will be provided to another group. Due to this discrimination opposite feedback of two groups is achieved whereas the server was honest in providing the services to all the nodes without any discrimination. In this type of attack, a single node may generate multiple fake IDs, and these IDs are used to give false recommendations about a targeted node.

2.6.15 Value Imbalance Exploitation Attack

If a malicious node in a network is able to provide high value to a low-quality service and vice versa it is called a value imbalance exploitation attack. A Value Imbalance Exploitation Attack is a type of cyber attack that leverages disparities between the perceived value of a service and its actual quality. In this attack, a malicious node manipulates the value and quality attributes to gain an unfair advantage within a network or system. The attacker aims to exploit the discrepancy between what is expected by network participants and the actual outcomes delivered.

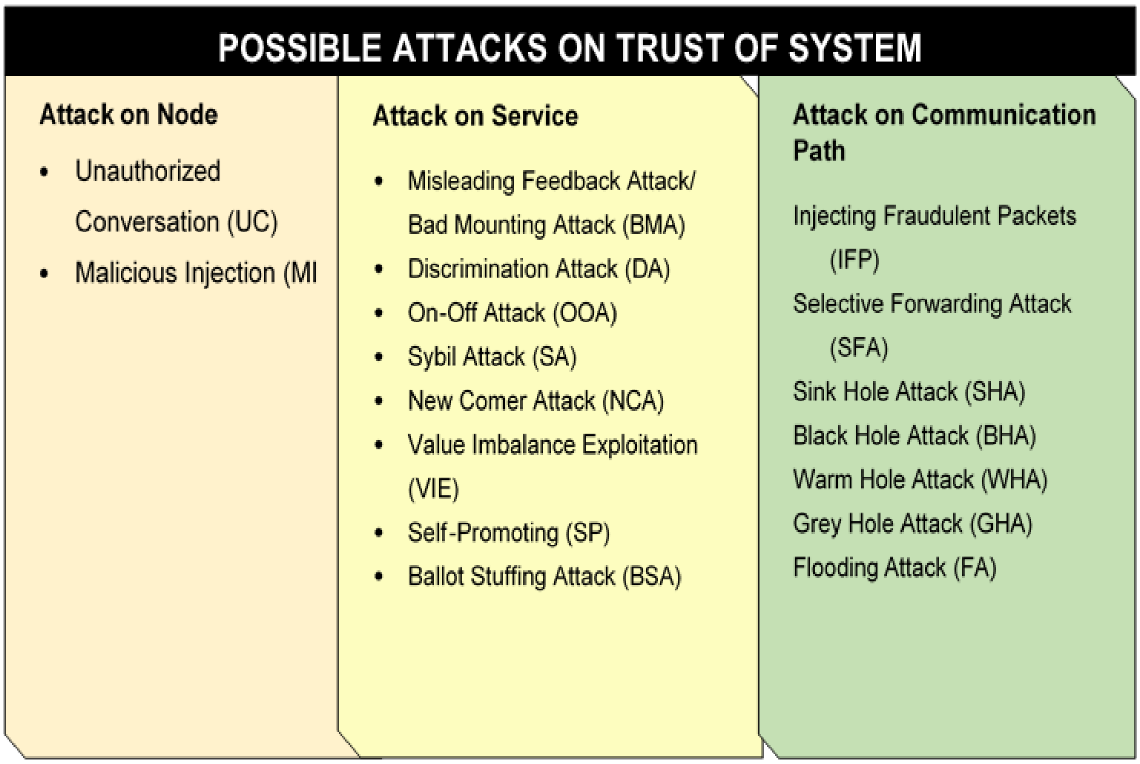
2.6.16 Unauthorized Conversation

In this type of attack, a node starts sending packets to other unauthorized nodes instead of a single legitimate node. An Unauthorized Conversation Attack is a type of cyber attack that occurs when two or more unauthorized nodes engage in communication or data exchange within a network or system without proper authentication or authorization. This type of attack violates the security policies and access controls of the network, potentially leading to information leakage, data breaches, or unauthorized access to sensitive resources.

2.6.17 Malicious Injection

Malicious Injection, also known as Data Injection Attack, is a type of cyber attack where an attacker gains control over a node within a network and then uses that compromised node to inject false or malicious data into the network. This attack aims to manipulate the integrity, authenticity, or accuracy of data being transmitted within the network, potentially leading to misinformation, system disruption, or exploitation of vulnerabilities. Figure 2.3 depicts the classification of all possible attacks on the trust of a system.

The relevance of different blockchains in the context of trust in smart systems lies in their ability to provide secure, transparent, and decentralized mechanisms for establishing, verifying, and maintaining trust. The choice of blockchain platform should align with the specific requirements and objectives of the smart system to maximize its impact on enhancing trust. Smart systems, which encompass various domains such as



POSSIBLE ATTACKS ON TRUST OF SYSTEM

Attack on Node

- Unauthorized Conversation (UC)
- Malicious Injection (MI

Attack on Service

- Misleading Feedback Attack/ Bad Mounting Attack (BMA)
- Discrimination Attack (DA)
- On-Off Attack (OOA)
- Sybil Attack (SA)
- New Comer Attack (NCA)
- Value Imbalance Exploitation (VIE)
- Self-Promoting (SP)
- Ballot Stuffing Attack (BSA)

Attack on Communication Path

Injecting Fraudulent Packets (IFP)
Selective Forwarding Attack (SFA)
Sink Hole Attack (SHA)
Black Hole Attack (BHA)
Warm Hole Attack (WHA)
Grey Hole Attack (GHA)
Flooding Attack (FA)

Figure 2.3: Classification of possible attacks on trust of a system

healthcare, supply chain, energy, and more, rely on efficient and trustworthy interactions among autonomous entities. It is possible through the usage of blockchain.

2.7 Current Blockchain Architectures

Blockchain is a distributed ledger [9] for the storage of transactions. It cannot be modified once populated by all concerned nodes. After its emergence, blockchain has totally changed the thoughts of human beings. Its unchallengeable integrity has provided it a basis to serve for decentralized finance where no third party like banks is required as a guarantor. It has given rise to cryptocurrency and there are more than 20,000 different kinds of crypto coins circulating in the digital market. In addition to the provision of confidentiality, Integrity, and availability, Blockchain has also provided authentication and non-repudiation.
Different blockchain platforms offer distinct features and capabilities that can enhance trust within smart systems:-

- Security and Immutability:- Block-chains provide a tamper-resistant and immutable ledger, ensuring that data once recorded cannot be altered without consensus. This feature enhances data integrity and prevents unauthorized modifications, which is crucial for building 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.

A few of the salient blockchain architectures currently in vogue are as under: -

2.7.1 Bit Coin

It is the most common blockchain known to every person nowadays. Bitcoin blockchain is a digital, decentralized, and secure way of keeping track of who owns how much Bitcoin and who is sending it to whom. It’s like a shared record book that lots of people help update and protect, making sure everything is honest and accurate. The

Bitcoin blockchain is the foundational technology behind the digital cryptocurrency Bitcoin. It's a decentralized and distributed public ledger that records all transactions made with Bitcoin. Unlike traditional financial systems, where a central authority (like a bank) verifies and maintains transaction records, the Bitcoin blockchain relies on a network of participants to collectively validate and record transactions.

2.7.2 Ethereum

Ethereum is another type of blockchain, similar to Bitcoin's blockchain but with some important differences. Like Bitcoin, Ethereum is a decentralized digital platform that allows people to send and receive a digital currency called Ether (ETH). However, Ethereum's blockchain is designed to do much more than just handle transactions. Ethereum introduced the concept of "smart contracts." These are like self-executing agreements with the rules directly written into code. They automatically execute and enforce the terms of an agreement when certain conditions are met. For example, you could create a smart contract to automatically release funds to a seller when a shipment is confirmed as delivered. while Bitcoin primarily focuses on being a digital currency and a store of value, Ethereum is a platform for building decentralized applications and executing complex smart contracts. It's designed to provide more flexibility and functionality beyond simple transactions, making it a versatile platform for various types of blockchain-based projects.

2.7.3 Hyper-ledger Fabric

Hyperledger Fabric is a blockchain framework that is part of the Hyperledger project, which is hosted by the Linux Foundation. It is designed to enable businesses to build and deploy private, permissioned blockchain networks for various enterprise use cases. Hyperledger Fabric provides a modular and customizable architecture that allows organizations to create blockchain solutions tailored to their specific needs. Fabric introduces the concept of "channels," which are sub-networks within the main blockchain network. Channels allow different groups of participants to have separate and private communication and transactions while sharing the same underlying blockchain infrastructure. The fabric uses a concept called "chain code" for smart contracts. Chaincode is written in familiar programming languages like Go, Node.js, or Java, which makes it more accessible to developers with diverse skill sets. Hyperledger Fabric is designed for high performance and scalability, making it suitable for enterprise-level applications. It supports parallel transaction execution, allowing multiple transactions to be processed simultaneously.

2.7.4 IOTA

IOTA is a unique distributed ledger technology that goes beyond the traditional blockchain architecture. It aims to address some of the limitations of traditional blockchains, particularly in terms of scalability, transaction fees, and energy efficiency. IOTA uses a technology called the Tangle, which is a Directed Acyclic Graph (DAG) structure, to achieve its goals. Unlike traditional blockchains that organize transactions into blocks, the Tangle uses a DAG structure. In the Tangle, each transaction is linked to multiple previous transactions, forming a web-like structure. This eliminates the need for miners and allows transactions to be verified by approving other transactions. This design aims to improve scalability as more transactions can be processed in parallel. In traditional blockchains, miners compete to add blocks to the chain, and users pay transaction fees to incentivize miners. In the IOTA Tangle, users themselves validate transactions by confirming other transactions. This eliminates the need for miners and transaction fees, which can lead to cost savings and faster transactions. Tangle's structure theoretically allows it to become faster and more scalable as more participants join the network. As more users make transactions, they contribute to the validation of other transactions, creating a self-sustaining and efficient network.

Chapter 3

Related Work/ Literature Review

Literature available on trust shows that very few researchers have worked with context-based or adaptive trust [10]. Blockchain has been used by no one for calculations and storage of trust to avoid integrity attacks. Table Number 3.1 shows trust management using blockchain.

Table 3.1: Trust management using blockchain

Ref	***Title***	***Context Based Trust***	***Trust Type***	***Year***	***Trust in***	***BlockChain used***
[11]	A block chain-based Trust System for the Internet of Things	No	De-centralized	2019	IoT	Terms and Obligations
[12]	A Trust Architecture for Blockchain in IoT	No	Centralized	2018	IoT	Data Source reputation and Gateway reputation

Continued on next page

Table 3.1 – *Continued from previous page*

Ref	*Title*	*Context Based Trust*	*Trust Type*	*Year*	*Trust in*	*BlockChain used*
[13]	Block chain-based Decentralized Trust Management in Vehicular Networks	No	De-centralized	2018	Vehicular system	RSU saving data about road conditions, road congestion or free roads
[14]	Blockchain based distributed management system for trust in VANETs	No	De-centralized	2021	Vehicular system	Routing information is saved on the blockchain to avoid tempering and traceability.
[15]	Trust Chain: Trust Management in Block chain and IoT supported Supply Chains	No	De-centralized	2019	Supply chain system	Interactions among supply chain participants, dynamic trust scores based on these interactions
[16]	A blockchain based Trust Model for IoT-Supply chain Management	No	De-centralized	2021	Supply chain system	Data of supply chain saved on blockchain effectively reducing latency, computational requirements and storage requirements
[17]	Strengthening the Blockchain based Internet of value with trust	No	De-centralized	2015	Data Network	Ownership of Assets is registered and saved with Blockchain to avoid any double spending of any assets

Continued on next page

Table 3.1 – *Continued from previous page*

Ref	***Title***	***Context Based Trust***	***Trust Type***	***Year***	***Trust in***	***BlockChain used***
[18]	Data Trust framework using blockchain technology and adaptive transaction validation	No	Decentralized	2021	Data Network	Defines 8 essential parameters for a trust management framework, Trust value of a data-set is calculated in terms of reputation, endorsement and confidence using three different Smart contracts, Similarly 3 x different smarts contracts are used for Access, provenance and consent management.
[19]	Early Access context based adaptive fog computing trust solution for time critical smart health care systems	Yes	Decentralized	2023	Trust Management in Fog	Blockchain is not used for saving or calculating the trust values.

3.1 Trust of IoT based Smart System

It is evident from Table 3.1 that research work is available in which blockchain has been used for provision of trust. However, it lacks context-based trust calculations. For example, at [11] and [12] centralized and decentralized Blockchain-based trust system of IoT is described respectively but, in [11] only terms and obligations defined by the service provider originally, are stored in blockchain, so that any service requester may

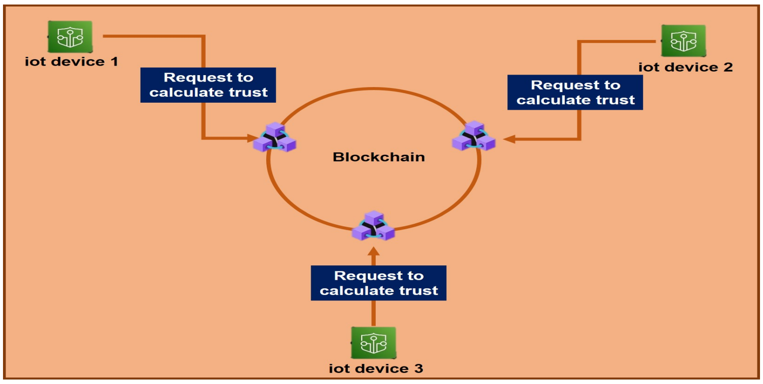

iot device 1
Request to calculate trust
iot device 2
Request to calculate trust
Blockchain
Request to calculate trust
iot device 3

Figure 3.1: Trust calculation of IoT devices using blockchain

go to blockchain and get the original copy of terms and obligation at the time of getting the services from the service provider. Blockchain is just ensuring the avoidance of modification of terms and obligations, there is no context-based trust being calculated. Similarly in [12] Trust is ensured by saving the confidence of the data source and reputation of the data source on blockchain and the provision of trust is on the basis of non-modifications of these stored values. However, No trust calculation of IoT devices or nodes interacting with each other is done for the avoidance of compromise of IoT devices or nodes.

3.2 Trust of Vehicular Smart System

A Vehicular Smart System, also known as a Vehicular Smart Network or Vehicular Ad Hoc Network (VANET), refers to a technology that enables communication and data exchange between vehicles and roadside infrastructure. It leverages wireless communication and sensor technologies to create a connected environment within the transportation system, allowing vehicles to share real-time information, such as traffic conditions, road hazards, and safety alerts. [20] At [13] A vehicular system is described comprising vehicles and RSUs (Roadside units). Messages received by any vehicle are confirmed from nearby other vehicles. If a positive response is achieved the reputation of the vehicle is upgraded and data is sent to RSUs for calculation of trust values of the concerned vehicle. Similarly, at [14] again a vehicular smart system is discussed. The reliability of messages exchanged is ensured by saving routing information on the blockchain to protect it from tampering and traceability. In both systems, trust of message exchanging devices is not calculated nor saved on blockchain to enhance the trust of the devices, hence overall trust of smart vehicular system.

3.3 Trust of Supply chain Smart System

A Supply Chain Smart System refers to the integration of advanced technologies and digital solutions to optimize and enhance various aspects of supply chain management. It leverages digitization, data analytics, and real-time communication to create a more efficient, transparent, and responsive supply chain ecosystem. The goal of a supply chain smart system is to improve visibility, coordination, and decision-making across the entire supply chain, from raw material suppliers to end consumers. A Supply Chain Smart System can result in improved operational efficiency, reduced costs, enhanced customer satisfaction, and increased competitiveness for businesses. At [15] Designer leverages smart contracts for automation of reputation calculation with Blockchain transactions and penalties to action the rewards and accountability for both supply chain participants and quality of food product being traded. Based on the output of the smart contracts, supply chain participants and commodities receive reputation scores as a measure of their trustworthiness for a trade event. Supply chain participants are then penalized by revoking their participation in the supply chain or rewarded by getting high ratings published. Similarly, at [16] Researcher proposes combining IoT and blockchain technology to solve the challenges of trust between supply chain parties and preserve data integrity. A blockchain offers a pathway to developing IoT technology that can facilitate the sharing of information that every party can see and trust. Each source of data is always visible, which makes the shared data secure and guaranteed. If large volumes of information have to be circulated among various members in various systems, such integration would prove useful. Data from the supply chain is saved on blockchain effectively reducing latency, computational requirements, and storage requirements. However, Above discussed both types of research lack calculation of trust of sensing devices for overall enhancement of trust of supply chain smart system.

3.4 Trust of Data Network Smart System

A Data Network Smart System refers to an advanced and interconnected network infrastructure that utilizes intelligent technologies to manage, transmit, and process data efficiently and effectively. This system leverages various digital solutions, automation, and optimization techniques to create a seamless and intelligent data communication environment. At [17] a Data Network is discussed in which ownership of assets is registered and saved with Blockchain to avoid any double spending of any assets. In this way, trust of a data network is enhanced without trust calculations of individual devices. Similarly, at [18] 8 essential parameters for a trust management framework are defined:-

1. Discovery:- It refers to the process of discovering the quality and properties of data by data users in the first phase.
2. Provenance:- It refers to the ability of data users to access the historical record and metadata about the data
3. Access controls:- Ability of data owners to control and manage access permissions toward their data
4. Access:- Refers to the mechanism that provide access for data users
5. Identity Management:- Ability of data owners to identify and authenticate data users
6. Auditing of use:- refers to providing a transparent history of data usage
7. Accountability:- refers to achieving accountability by access control and auditing of use.
8. Impact:- refers to assessing the value, usage and misuse of data through recorded information in data trust.

Moreover, trust value of a data-set is calculated in terms of reputation, endorsement and confidence using three different Smart contracts, Similarly 3 x different smarts contracts are used for Access, provenance and consent management.

3.5 Trust of Health Care Smart System

A Healthcare Smart System refers to the integration of advanced technologies and digital solutions to optimize and enhance various aspects of healthcare delivery, management, and patient experience. It leverages digitization, data analytics, and real-time communication to create a more efficient, patient-centered, and technology-driven healthcare ecosystem.A Healthcare Smart System aims to improve patient outcomes, enhance the efficiency of healthcare operations, and empower patients to take a more active role in their health. By leveraging technology and data-driven insights, healthcare organizations can provide better care, reduce costs, and create a more patient-enteric and sustainable healthcare ecosystem. At [19] A smart health care system utilizing fog is discussed. In this research work, context-based trust of nodes is calculated, However, Trust is not calculated using blockchain nor saved on the blockchain.

In all the above research works, adaptive trust is not calculated nor saved on the blockchain for better trust of smart systems. All these trust solutions are vulnerable to integrity attacks. If the total trust of any Service provider calculated by any node is modified by any malicious node, it will cause a bad-mouthing attack for that specific Service provider Node. Table number 3.2 summarizes a brief comparison of Context-based trust work so far available.

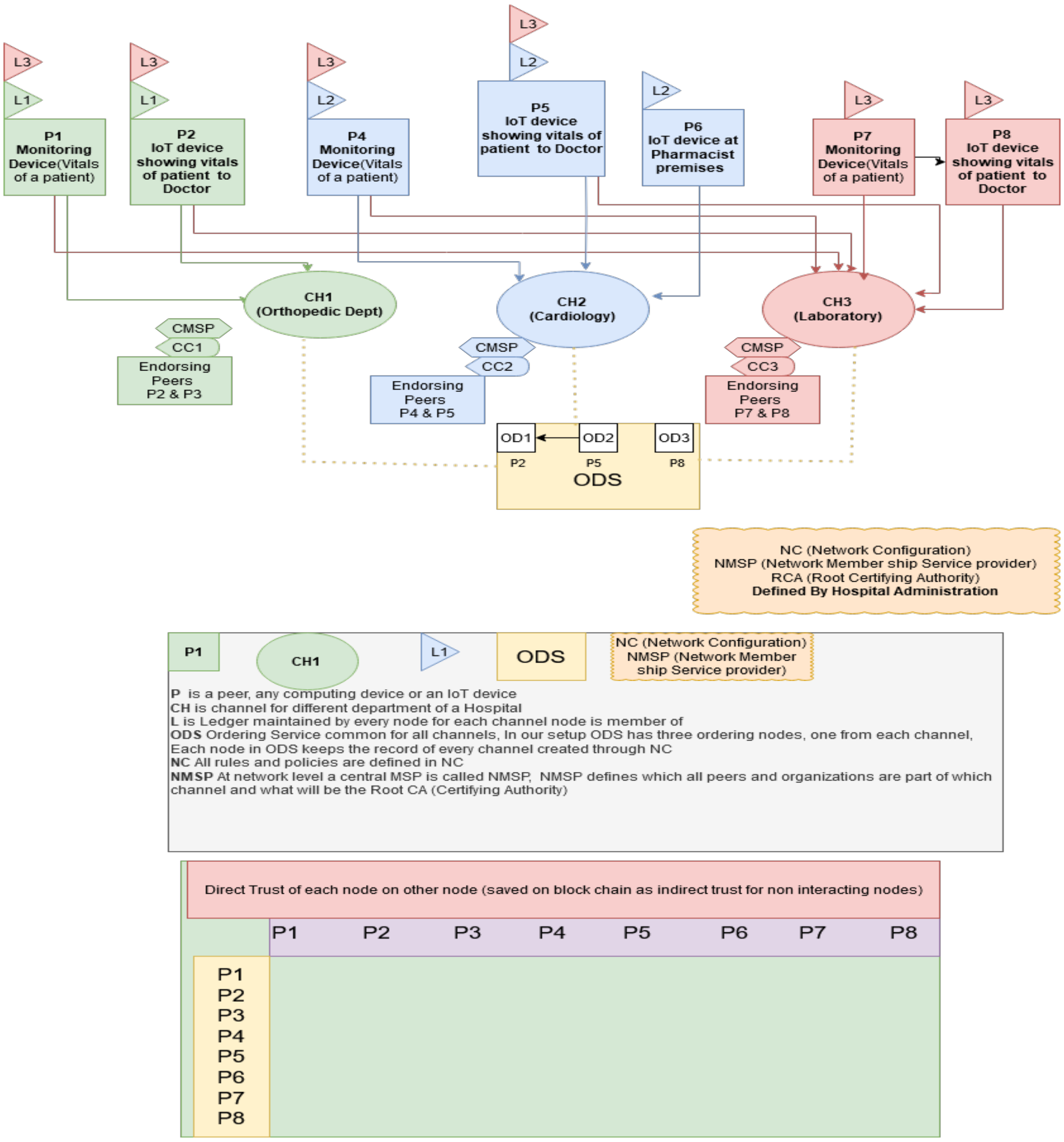
Table 3.2: Comparison of context based trust work

Ref	**Specifications**				
	Context Based Trust	***Centralized/ De-centralized Trust***	***Attacks Covered***	***Simulation***	***Trust stored on Blockchain***
[21]	Yes	De-centralized	Nil	Nil	Nil
[7]	Yes	De-centralized	On Off attacks, sybil attacks	Contiki Cooja Plateform	Nil
[22]	Yes	De-centralized	Nil	Contiki Cooja Plateform	Nil
[8]	Yes	De-centralized	Ballot Stuffing Attack, Bad Mouthing Attack	Nil	Nil

Chapter 4

Trust in Healthcare System - A Case Study

Let's consider a case study involving the calculation of trust for IoT devices attached to a healthcare system. we will explore how trust may be assured and managed for various IoT devices used in a hospital environment. A private hospital may have implemented an IoT-based healthcare system to monitor patients' vital signs remotely and ensure timely medical interventions. The system includes various IoT devices, such as wearable sensors, bedside monitors, and medical imaging equipment. The goal is to calculate and manage the trustworthiness of these IoT devices to ensure the accuracy and security of patient data and enable informed decision-making by healthcare professionals. we will develop a prototype trust management system that aggregates the calculated trust factors for each IoT device and assigns an overall trust score to each device. The trust score can be displayed to healthcare professionals and administrators, indicating the level of confidence in each device's data. Real-time monitoring and alerting mechanisms can be implemented that trigger notifications if a device's trust score falls below a predefined threshold. Remediation actions can include temporarily disabling the device, initiating diagnostics, and notifying the IT or biomedical engineering team for further investigation. By calculating and managing trust in IoT devices within the healthcare system using blockchain, hospitals can ensure patient safety, data integrity, and regulatory compliance, thereby enhancing the overall quality of patient care. It will work as under:-



P is a peer, any computing device or an IoT device
CH is channel for different department of a Hospital
L is Ledger maintained by every node for each channel node is member of
ODS Ordering Service common for all channels, In our setup ODS has three ordering nodes, one from each channel, Each node in ODS keeps the record of every channel created through NC
NC All rules and policies are defined in NC
NMSP At network level a central MSP is called NMSP, NMSP defines which all peers and organizations are part of which channel and what will be the Root CA (Certifying Authority)

Direct Trust of each node on other node (saved on block chain as indirect trust for non interacting nodes)

	P1	P2	P3	P4	P5	P6	P7	P8
P1								
P2								
P3								
P4								
P5								
P6								
P7								
P8								

Figure 4.1: Trust Management using Hyper Ledger Fabric

4.1 Device Identity and Registration

Each IoT device is registered on the blockchain network as a unique identity. smart contracts are deployed to verify device authenticity and ensure that only authorized devices can join the network.

4.2 Data Collection

IoT devices transmit selected trust parameter values to the blockchain. Smart contracts record data to ensure the integrity of data.

4.3 Trust calculation and storage

Trust parameters, such as response time, Latency, and packet loss ratio, are defined as attributes in the blockchain network. Based on these parameters aggregate trust of each IoT device will be calculated through a smart contract. Block-chain's tamper-resistant ledger ensures that once trust scores are recorded, they cannot be altered without consensus from the network.

4.4 Privacy and Access Control

Private blockchain's permissioned network model allows granular access control to ensure that only authorized healthcare personnel can view and interact with trust-related data.

4.5 Data Integrity and Immutability

Blockchain is known for its ability to create a tamper-resistant and immutable ledger of transactions. In the context of IoT, this can help ensure the integrity of trust calculated for various devices. Once calculated and recorded, it becomes extremely difficult to alter or tamper with the trust value, thereby increasing trust in the accuracy and authenticity of the information.

4.6 Decentralization and Security

Trust values of IoT devices and nodes are being calculated centrally. By using a decentralized blockchain, the reliance on a single point of control is reduced, making it harder for malicious actors to compromise the network. Blockchain's cryptographic techniques also enhance data security and authentication, reducing the risk of unauthorized access and ensuring that only authorized devices can participate in the network.

4.7 Smart Contracts for Automation

Smart contracts are self-executing contracts with predefined rules and conditions. They can automate various processes in IoT ecosystems, such as device-to-device transactions, data sharing, and payments. This automation can reduce the need for intermediaries, streamline processes, and minimize the potential for errors or disputes, further enhancing trust among IoT devices.

4.8 Alerts

Smart contracts will trigger alerts or notifications when a device's trust score falls below a certain threshold, prompting healthcare staff to take action. By utilizing blockchain to calculate and manage trust for IoT devices in a healthcare system, the hospital can enhance patient care, ensure data accuracy, and maintain a secure and transparent environment for medical IoT device operations. Figure 4.2 describes the calculation of trust of IoT devices using blockchain. In this way, a Smart system getting total trust values through blockchain will be more secure and less vulnerable to integrity attacks.

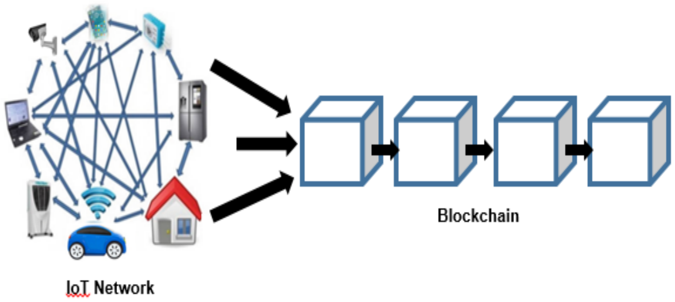


Figure 4.2: Trust calculation and preserving of Trust using blockchain

Chapter 5

Proposed Solution and Architecture

Trust values of IoT devices calculated centrally or decentrally are under continuous threat and are vulnerable to integrity attacks as they are not saved on the blockchain. To avoid, compromising trust values, Blockchain technology can play a significant role in enhancing the calculation and ensuring the trustworthiness of IoT devices. Blockchain technology can enhance the calculation and preservation of trust in IoT devices by providing data integrity, security, automation, consensus, traceability, and identity management. These features can collectively contribute to a more reliable and secure IoT ecosystem, fostering greater confidence among both users and stakeholders.

Resultantly, we are motivated to apply blockchain to play its role to calculate and save trust values of legitimate nodes to avoid integrity attacks. Hence, Trust values will be calculated using blockchain and will be stored on the blockchain.

5.1 Selection of Blockchain

For calculation/storage of trust which type of blockchain is better and more advantageous? It is the next question in our journey of proposing a solution. Different types of blockchain are available. Public and private. In our scenario, which type of blockchain will be more useful? A detailed comparison of public and private blockchains is obvious from Table 5.1.

Table 5.1: Comparison of private and public blockchain

Ser No	Feature	Private Blockchain	Public Blockchain
1	Decentralized	Yes(For part of Organization)	Yes
2	Same Ledger	No	Yes
3	Immutable	Yes	Yes
4	Anonymous	No	Yes
5	All Node Verification	No (Endorsing Nodes Only)	Yes
6	Transparent	No	Yes
7	Smart Contract	Yes	Yes

5.1.1 Public Blockchain Issues

Having a detailed comparison of a public and private blockchain, we came to know that public blockchain has the following three fundamental issues, which create a hindrance for the private sector to make use of it.

- Confidentiality:- Data is shared and available with every full node. All transactions are transparent for every participating node, not acceptable for a private company.
- Slow:- To mine and publish a transaction, every node participates and transactions are verified and then published. In Bitcoin, a block takes a minimum of 10 minutes to publish a block. In the Proof of Work protocol, solving the hash puzzle is time-consuming and makes the blockchain slow. However, in the private sector, a relatively fast blockchain is required. Figure 5.1 shows a comparison of different blockchain transactions with Visa and Paypal.
- Scalability:- Size of chain is ever increasing. From the genesis block till the last block published, thousands of blocks are there. All these blocks are required to be downloaded by at least a Full Node for verification purposes and to be synchronized with all other nodes.

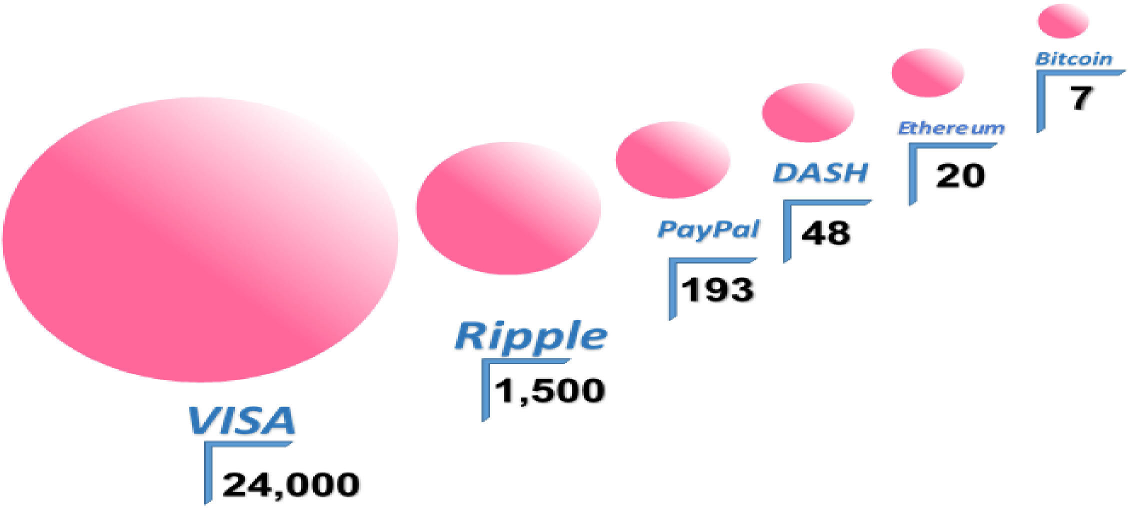


Figure 5.1: Cryptocurrencies Transaction Speeds Comparison with Visa and PayPal

5.2 Why Hyper Ledger Fabric

More specifically, we will now explore our case study involving the calculation of trust for IoT devices attached to a healthcare system using the Hyperledger Fabric blockchain. We will focus on how Hyperledger Fabric's features can enhance trust calculation and management for IoT devices in a healthcare environment. The aim is to leverage Hyperledger Fabric to establish a secure, transparent, and tamper-resistant trust calculation mechanism for IoT devices, ensuring the accuracy and reliability of patient data. In our scenario, HLF is considered to be more effective instead of any public blockchain. HLF being a private ledger, is more suitable for nodes interacting with each other, and having fewer resources. IoT devices are always having less computational power, less memory, and less backup time. So instead of having a Public blockchain like Ethereum, requiring the participation of each node 24/7. HLF requires a Network of nodes of committing, Endorsing, and Ordering service peers for its functioning. All nodes are part of HLF as committing peers but for 24/7 working endorsing peers and ODS are required only. Few Nodes with more computational power, memory, and backup time can be assigned the duties of endorsing peers and ordering service peers. Rest all nodes may act as normal clients and may revoke a smart contract, whenever they need services of blockchain.
Figure 4.1 explains the detailed Hyper Ledger Fabric structure of a Trust management system of IoT devices of a private hospital.

5.2.1 Installation of Test Network of HLF

Detailed information about HLF is available on the following link:-
https://hyperledger-fabric.readthedocs.io/en/release-2.5/ The Following Steps are performed for installation of HLF:-

- Installation of Ubuntu:- Ubuntu was installed on windows using virtual box.
- Curl Installation:- Version 7.68.0 of curl was installed on Ubuntu.
- Node JS Installation:- Version 10.19.0 of Node JS was installed on Ubuntu. Any version till 10 or above was the minimum required for HLF.
- Git Installation:- Version 2.25.1 of Git was installed on Ubuntu.
- Python Installation:- Version 3.8.10 of python was installed on Ubuntu.
- Docker Installation:- Version 20.10.24 of Docker was installed on Ubuntu.
- Docker-compose Installation:- Version 1.29.2 was installed on Ubuntu.

5.3 Proposed HLF Architecture

In a private hospital Hyper Ledger Fabric will be best best-suited blockchain type for calculation and preservation of trust values. As shown in figure number 4.1, A hospital comprising the Orthopedic Department, Cardiology Department, and Laboratory is considered.

5.3.1 Channels and CA

Each department has its own blockchain running separately. In HLF It is called channel. Each department is assigned a separate channel. Each channel has its Certifying authority as well. Any node or peer, wanting to interact with the blockchain has to be registered and enrolled with the CA of that channel. In this way, the privacy and secrecy of departmental data is ensured. A node/peer not registered to a channel is not authorized and not given access to data present on a channel of a specific department. Hence, a strong Access control mechanism is ensured to avoid all identify-based attacks like Sybil attacks, etc.

Different peer parts of a channel are divided into different categories. No peer can go beyond its authorization.

5.3.2 Endorsing peers

These peers are responsible for checking off a chain code or a smart contract. Endorsing peers will run the chain code and will observe the expected outcome of a chain code. If the outcome of more than one endorsing peer (No of peers required to be agreed on a chain code is defined in initial configuration) is the same as per expectation. Endorsing peers will confirm the legitimacy of a chain code. Code will be deployed and run on that channel. Endorsing peers in this way will ensure that no malicious code is executed on the Blockchain. Hence, the running of legitimate code on the desired channel is ensured.

5.3.3 Ordering peers

It is proposed that at least one peer per channel should act as an ordering peer. Ordering peers will ensure the correct sequencing of blocks being committed on a channel. Correct sequencing can help us to track the desired block easily.

5.3.4 Committing Peers

It is proposed that peers other than endorsing or ordering peers all other peers and user applications must be committing peers. It must be registered with the CA of the channel. Once a chain code or smart contract is invoked or triggered by any committing node. Already endorsed and authorized chain code is run and required output is generated. Few values of trust parameters are required to chain code as input and trust value will be generated by Blockchain as output. Output value of trust will be stored on the Blockchain. In this way, blocks having transactions in them, are sent to ODS for being committed to Blockchain. Once a block is committed and made part of Blockchain, is never changed.

5.3.5 Chain Code/smart contract

A chain code or a smart contract is the same thing. It is a piece of code designed to do our desired task. in our scenario, chain code will calculate and store the trust of any node, whose services are required.

5.4 Proposed Trust Parameters

Chain code will calculate trust from the values provided. Out of so many trust parameters, the following proposed trust parameters will be taken as input to calculate the trust.

- Response Time:- Time taken to send a request and reply of the request is received back to the requester is called response time. Lessor the time response time, the more the trust of the responder.
- Packet loss ratio:- The ratio of the packets lost in the way to the total packets sent is called packet loss ratio. Lessor the packer loss ratio, the more the trust value of the packet sender.
- Latency:- Latency is the time required for a packet to traverse among two different nodes. Less the latency, the more will be the trust of a specific node sending the packets.

The above three values will be taken as input by the smart contract and will be used for the calculation of trust. As there is no universal formula for the calculation of trust. The following proposed formula will be used for the calculation of trust

$$T = j * k + l * m + n * o \tag{5.4.1}$$

where
T = Trust value of any node being calculated;
j = Weight-age of 1st Trust Parameter, how much part this parameter plays in calculation of overall trust value;
k = 1st parameter itself i.e. response time;
Similarly
l = Weight-age of 2nd Trust Parameter;
m = 2nd Parameter;
n = Weight-age of 3rd Trust Parameter;
0 = 3rd parameter;

and

j = 0.5;

k = Response time;

l = 0.3;

m = Packet loss Ratio;

n = 0.2;

o = Latency;

In this way, trust will be calculated using a blockchain smart contract. Trust will be stored in the Blockchain as the Direct trust. For example, Direct trust of P1 on P4. The same value of the direct trust will serve as an indirect trust for other nodes. i.e. P2, P3, P5, and P6.

Chapter 6

Analysis and Results

6.1 Limitation of Experimental Setup

In a real system, IoT devices are required to provide trust parameter values to the blockchain for the calculation of trust after each interaction with any other device. IoT devices in our scenario are not real but are simulated. A random number generator function is used to randomly generate values of trust parameters i.e. Latency, Response time, and Packet loss ratio just like the actual IoT devices. These values are fed to the smart contract and trust values are calculated by blockchain.

6.2 Invoking of Smart Contract

In this setup, 10 IoT devices having different locations and types of services are enrolled with the CA of respective channels. These devices interact with smart contracts as a client and invoke smart contracts, that is already endorsed by endorsers and installed on the blockchain. Each time a device invokes a smart contract a previously saved direct trust value is acquired from the blockchain. If no direct trust value is available with blockchain, It will go for the indirect Trust value. Here, comes the adaptive trust, where Blockchain checks the similarities of recommenders and the device asking for trust value. If the location and type of service of the requester and recommenders are matched. All those values are fetched and the average value of all the similar recommenders is calculated as the indirect trust. Now Total trust is calculated by adding Direct trust and Indirect trust. In an exceptional case, if there is no trust value at all, neither direct nor indirect, then a neutral value of 0.5 is assigned to that node for the next interaction as an indirect trust value.

6.3 Thresholding of Trust Values

Trust values once received from blockchain is now available to the respective requester node/ IoT device. If the value is above 0.5, It will be a green signal for node to get services from that specific node. otherwise it will search for other node for the required services.

6.4 Avoidance of Trust-related Attacks

Trust values of interacting peers/IoT devices, once calculated and stored on the blockchain, are now saved from different threats. Now there are negligible chances of their modification. Integrity is preserved by blockchain, hence, no Integrity attacks are possible now. Blockchain's features such as immutability, consensus mechanisms, cryptographic security, and transparency collectively contribute to creating an environment that is resistant to various integrity attacks. In this section, we will analyze how effective are we in our implemented architecture and solution. What are the achieved results after the implementation of blockchain architecture?Blockchain technology employs a decentralized and transparent approach for achieving trust in various applications, including financial transactions, supply chain management, voting systems, and many more. The key features of blockchain that contribute to avoiding trust-related attacks are immutability, consensus mechanisms, and transparency. Blockchain will provide defence against following attacks:-

6.4.1 Bad Mouthing Attack

In a blockchain, The Direct 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 after the fact, thus preventing bad-mouthing attacks.

6.4.2 Ballot Stuffing Attack

In our implemented system, If a node has not interacted with another node earlier, it does not have the direct trust value of that node. It will ask other nodes to give their recommendations about that specific node. In a non-blockchain environment it is the place where a ballot stuffing attack can play its role and false recommendation of a malicious node can make it a legitimate node spoiling the overall trust of the system. But, in a blockchain-based recommendation system, each recommendation is recorded as a transaction on the blockchain. Since transactions are validated by consensus mechanisms, and each participant has a copy of the entire ledger, it becomes very difficult to add illegitimate recommendations without detection. The transparency of the blockchain ensures that everyone can verify the integrity of the recommendation process.

6.4.3 Sybil Attack

In Hyper Ledger Fabric the application user has to get himself registered and enrolled with the organization's certificate authority (CA). In this process of enrollment user receives the necessary cryptographic material, necessary to get authenticated by the network. Hyper Ledger Fabric blockchain networks use BFT consensus mechanisms to validate the transactions (Trust calculations). These consensus mechanisms require participants to prove their dedication to the network, making it expensive and resource-intensive to create multiple identities. Due to both above factors, Sybil attacks in our HLF-based system are impossible.

6.4.4 On-Off Attack

On-off attacks involve participants entering and leaving the network at specific times to manipulate the system. In a blockchain network, the consistency of the ledger is maintained through consensus mechanisms. If a participant enters or leaves the network, it would affect their ability to participate in the consensus process, making it harder to manipulate the system without detection. Hence On-Off attack is also best defended in our HLF-based architecture.

6.5 Avoidance of Oracle Problem

In any Blockchain-based system, The Oracle problem is an aggravated issue [23]. Blockchain provides a guarantee of data preservation after it has been entered into the blockchain. If data is modified before it is entered into the blockchain, then what will be the solution? In Our Scenario, data is being fed to the blockchain in the form of trust parameters like response time, latency, and packet loss ratio. It is a difficult task for an attacker to segregate the data interpret it and then manipulate it for its own purpose.
Even if all, data is manipulated by any attacker, we again have a remedy for it. We may ask for multiple trust parameter values from interacting nodes and at different times we may use different parameters for the calculation of trust. hence avoiding the Oracle Problem.

6.6 Efficiency of Implemented Solution

Formulated code was run for a considerable time and values of different parameters were noted to check the efficiency of the proposed solution. Data from more than 100 transactions was noted and the following graphs were made:-

6.6.1 Trust Value Execution Time

Another important factor in checking the efficacy of the proposed solution is the time taken to get a trust value. It is very important in a system where hundreds of the nodes are desiring to interact with one another. If the time taken to get a trust value is more, Nodes can not wait for a longer time to get trust values before making a connection with another node. More than 100 transactions data shows that the average time taken by Hyper Ledger fabric is not more than 2 seconds. 2 seconds time is a good time for a node to get the trust value of any node and decide whether the connection should be made or not. If the processing power of the blockchain running machine is increased it can be further reduced. Figure 6.1 shows the data of more than 100 transactions.

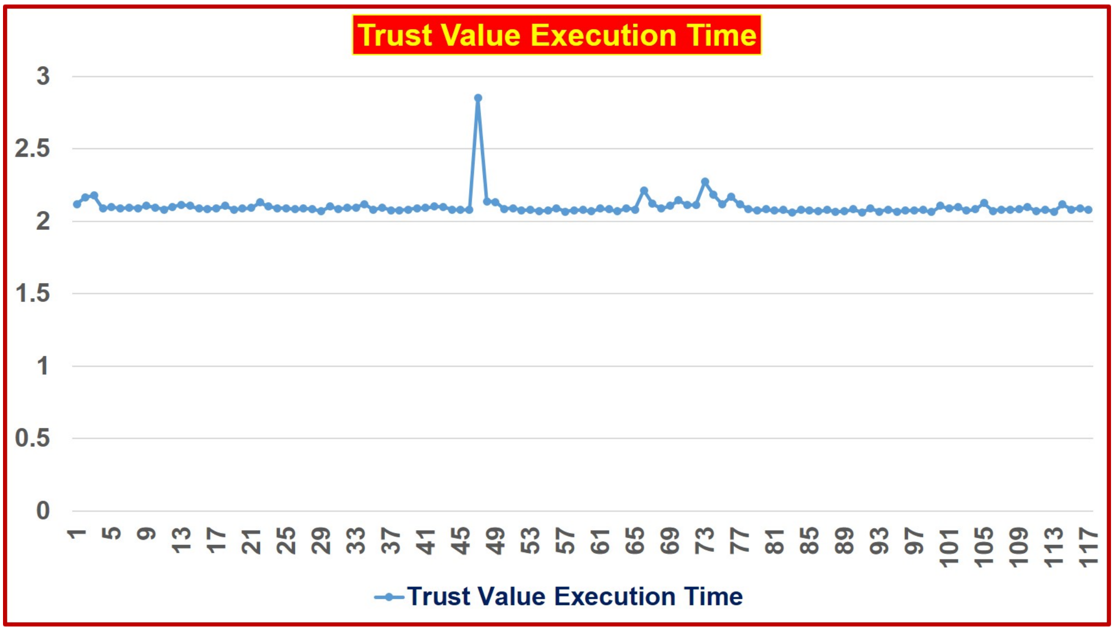


Figure 6.1: Trust Value Execution Time

6.6.2 Latency Vs Trust Values

It is evident from the graph between Latency and Trust values that a reverse relation between both parameters exists. Even the weight-age of latency is 20 percent towards the calculation of trust values. However, its impact on the calculation of trust values is obvious. The lower the latency more the trust value. Figure 6.2 shows the relation of latency and trust values calculated.

6.6.3 Response Time Vs Trust Values

Another parameter taken for the calculation of trust values was response time. The graph between response time and trust values also shows that an inverse relation between both parameters is present. Weight-age of response time is 50 percent as per the proposed formula. However, its impact on the calculation of trust values is very clear. The lower the response time more is the trust value. Figure 6.3 shows the relation of response time and trust values calculated.

6.6.4 Packet Loss ratio Vs Trust value

The number of packets lost in the communication path is a very important factor for the calculation of trust. If the packet loss ratio is higher, Trust values will be dropped

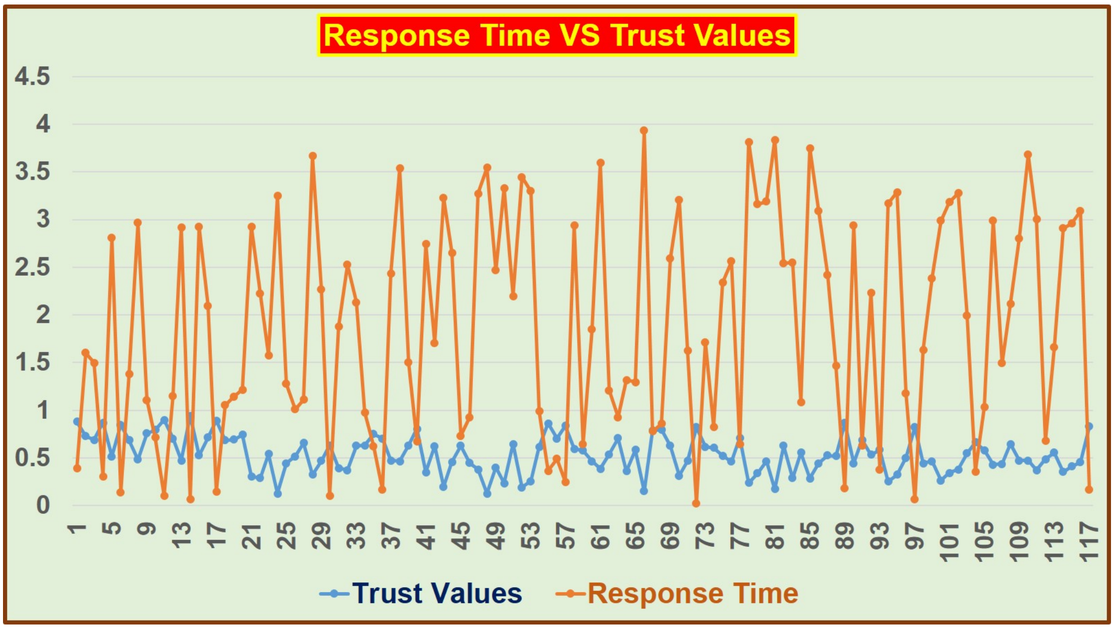


Figure 6.2: Latency Vs Trust values

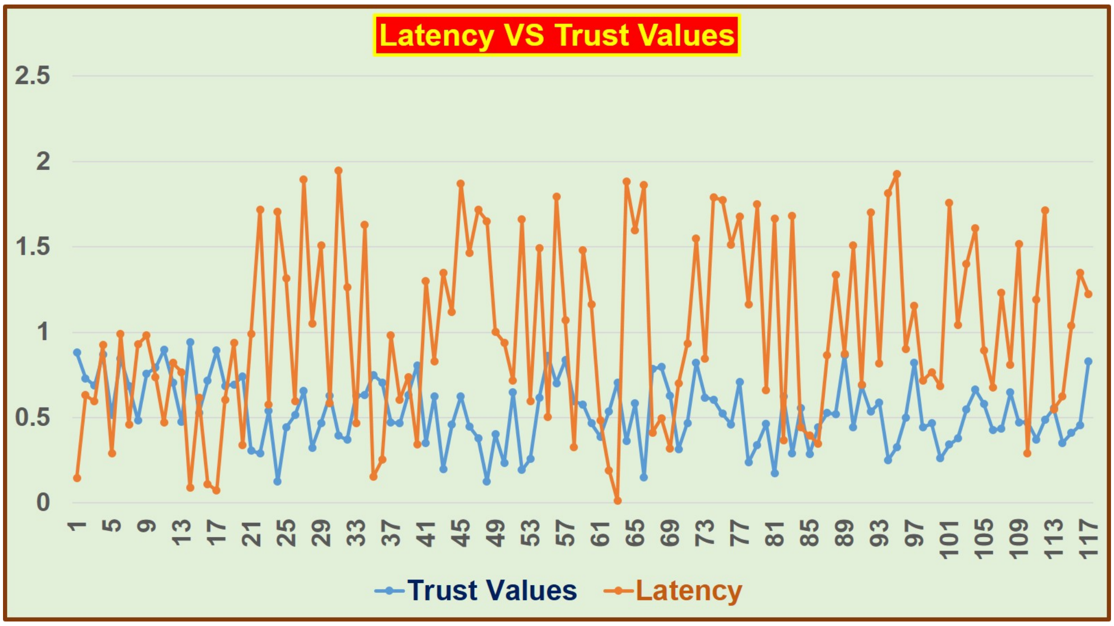


Figure 6.3: Response time Vs Trust values

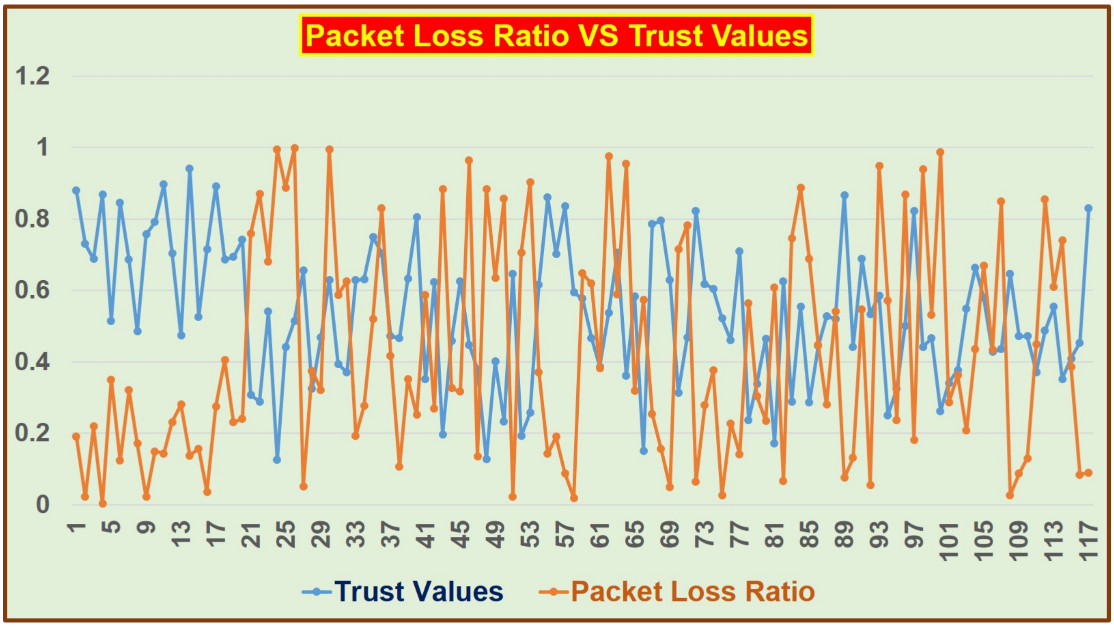


Figure 6.4: Packet Loss Ratio Vs Trust values

to zero. The same is evident from the graph showing the relation between packet loss and trust values. Figure 6.4 shows the relation of packet loss ratio and trust values calculated.

Chapter 7

Conclusion and Future Work

Trust is the most important aspect of now a day's smart world. Any existing smart system will collapse in no time if there is no element of trust. Context-based trust is real trust with enhanced value. Trust calculated with respect to the concerned context is more valuable and durable. The context-based trust calculation procedure is prone to integrity attacks by any malicious node. To avoid such types of attacks, total calculated trust is stored on the blockchain which cannot be modified by any malicious node. Blockchain-based trust is free of any integrity attack and is more secure.
Our investigation underscores the foundational role that cryptographic primitives play in fortifying the pillars of trust in smart systems. By integrating these primitives with the immutability and decentralization of blockchain, we have engineered a paradigm where trust is no longer reliant on centralized intermediaries, but rather on mathematical proofs and distributed consensus.

In establishing trust within smart systems, our findings reveal the potency of cryptographic protocols such as digital signatures, hashing, and encryption. These mechanisms are not only instrumental in securing communications and authenticating identities but also in the creation of tamper-resistant records that underpin the very essence of trust in a decentralized framework.

Furthermore, our work has cast light on the symbiotic relationship between cryptographic primitives and the broader ethos of blockchain, elucidating how their collaboration can address the multifaceted challenges that beset smart systems. We have substantiated the viability of our approach through concrete implementations and simulations, showcasing both the theoretical promise and real-world applicability of cryptographicpowered trust in diverse contexts.

However, we also acknowledge that our journey is but a prologue to the vast expanse that lies ahead. As the landscape of smart systems evolves, so too must our strategies for instilling trust and safeguarding data. Opportunities abound for deeper exploration of advanced cryptographic techniques, privacy-enhancing protocols, and novel consensus mechanisms that can usher in new dimensions of trust and security.

In conclusion, our endeavor to leverage the cryptographic primitives of blockchain for trust in smart systems has illuminated the path toward a more resilient, transparent, and decentralized future. By merging the power of mathematics with the potency of distributed ledgers, we have unveiled a landscape where trust is a product of collaboration between code, computation, and consensus. As we peer ahead, we are poised to embrace the challenges and discoveries that await on this dynamic journey of technological advancement and societal transformation.

7.1 Future work

7.1.1 Enhanced Trust Algorithms

The Trust Algorithm used was a simple weighted sum formula. Investigations and development of more advanced trust calculation algorithms that may take into account a wider range of parameters and factors, will be an enhancement of this work. Machine learning or AI-based approaches can also be considered to improve the accuracy of trust assessments.

7.1.2 Privacy-Preserving Trust Calculations

Explore methods for calculating trust without exposing sensitive device-specific information. Investigate privacy-preserving techniques, such as homomorphic encryption or zero-knowledge proofs, to ensure that trust calculations do not compromise privacy.

7.1.3 Integration with Consensus Mechanisms

Investigate how to integrate your trust calculation system with different consensus mechanisms within the Hyperledger Fabric framework. Explore how different consensus mechanisms impact the trust calculation process and the overall system performance.

7.1.4 Real-World Deployment and Testing

Conduct real-world testing and deployment of your system in an actual IoT environment. This could involve collaborating with industry partners or deploying the system in a controlled environment to gather more realistic data and insights.

7.1.5 Interoperability with Other Blockchains

Explore the potential for interoperability between your blockchain-based trust system and other blockchain networks. Investigate how trust values could be shared or verified across different blockchain platforms.

7.1.6 Decentralized Identity Management

Investigate how decentralized identity management solutions, such as self-sovereign identity, could enhance the trust calculation process. Explore the integration of decentralized identity frameworks with your existing system.

7.1.7 Economic Models for Incentives

Research and design economic models that incentivize honest behavior and participation in the IoT network. Explore token-based systems or other incentive mechanisms to reward trustworthy behavior.

Bibliography

[1] Imran Makhdoom et al. “Blockchain’s adoption in IoT: The challenges, and a way forward”. In: *Journal of Network and Computer Applications* 125 (2019), pp. 251–279.

[2] Liming Wang et al. “Trust Assessment in Internet of Things Using Blockchain and Machine Learning”. In: (2020).

[3] Imran Makhdoom et al. “PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities”. In: *Computers & Security* 88 (2020), p. 101653.

[4] Ayesha Altaf et al. “Trust models of internet of smart things: A survey, open issues, and future directions”. In: *Journal of Network and Computer Applications* 137 (2019), pp. 93–111.

[5] Qi Liu and Xiao Zou. “Research on trust mechanism of cooperation innovation with big data processing based on blockchain”. In: *EURASIP Journal on Wireless Communications and Networking* 2019.1 (2019), pp. 1–11.

[6] Mahnoor Hamza et al. “A social qualitative trust framework for Fog computing”. In: *Computers and Electrical Engineering* 102 (2022), p. 108195.

[7] Ayesha Altaf et al. “Mitigating service-oriented attacks using context-based trust for smart cities in IoT networks”. In: *Journal of Systems Architecture* 115 (2021), p. 102028.

[8] Ayesha Altaf et al. “Context-oriented trust computation model for industrial Internet of Things”. In: *Computers & Electrical Engineering* 92 (2021), p. 107123.

[9] Jiafu Wan et al. “A blockchain-based solution for enhancing security and privacy in smart factory”. In: *IEEE Transactions on Industrial Informatics* 15.6 (2019), pp. 3652–3660.

[10] Rajesh Kumar and Rewa Sharma. “Leveraging blockchain for ensuring trust in IoT: A survey”. In: *Journal of King Saud University-Computer and Information Sciences* 34.10 (2022), pp. 8599–8622.

[11] Roberto Di Pietro et al. “A blockchain-based trust system for the internet of things”. In: *Proceedings of the 23nd ACM on symposium on access control models and technologies.* 2018, pp. 77–83.

[12] Volkan Dedeoglu et al. “A trust architecture for blockchain in IoT”. In: *Proceedings of the 16th EAI international conference on mobile and ubiquitous systems: computing, networking and services.* 2019, pp. 190–199.

[13] Zhe Yang et al. “Blockchain-based decentralized trust management in vehicular networks”. In: *IEEE internet of things journal* 6.2 (2018), pp. 1495–1505.

[14] Youssef Inedjaren et al. “Blockchain-based distributed management system for trust in VANET”. In: *Vehicular Communications* 30 (2021), p. 100350.

[15] Sidra Malik et al. “Trustchain: Trust management in blockchain and iot supported supply chains”. In: *2019 IEEE International Conference on Blockchain (Blockchain).* IEEE. 2019, pp. 184–193.

[16] Mabrook S Al-Rakhami and Majed Al-Mashari. “A blockchain-based trust model for the internet of things supply chain management”. In: *Sensors* 21.5 (2021), p. 1759.

[17] Nguyen B Truong et al. “Strengthening the blockchain-based internet of value with trust”. In: *2018 IEEE international conference on communications (ICC).* IEEE. 2018, pp. 1–7.

[18] Sara Rouhani and Ralph Deters. “Data trust framework using blockchain technology and adaptive transaction validation”. In: *IEEE Access* 9 (2021), pp. 90379–90391.

[19] Aiman Almas et al. “Context-based adaptive Fog computing trust solution for time-critical smart healthcare systems”. In: *IEEE Internet of Things Journal* (2023).

[20] Chenyue Zhang et al. “AIT: An AI-enabled trust management system for vehicular networks using blockchain technology”. In: *IEEE Internet of Things Journal* 8.5 (2020), pp. 3157–3169.

[21] Ayesha Altaf, Haider Abbas, and Faiza Iqbal. “Context based trust formation using Direct User-Experience in the Internet of Things (IoT)”. In: *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE. 2019, pp. 424–430.

[22] Ayesha Altaf et al. “Robust, secure, and adaptive trust-oriented service selection in IoT-based smart buildings”. In: *IEEE Internet of Things Journal* 8.9 (2020), pp. 7497–7509.

[23] Ammar Hassan et al. “From trust to truth: Advancements in mitigating the Blockchain Oracle problem”. In: *Journal of Network and Computer Applications* 217 (2023), p. 103672.