Leveraging Cryptographic Primitives of Blockchain for Trust in Smart Systems

Hafiz Asif Khalil, Ammar Hassan*, Waseem Iqbal, Muhammad Atif Khalil
National University of Science and Technology, Islamabad, Pakistan
***Corresponding Author:** ammar.hassan@mcs.nust.edu.pk

Citation | Khalil. H. A, Hassan. A, Iqbal. W, Khalil. M. A, "Leveraging Cryptographic Primitives of Blockchain for Trust in Smart Systems", IJIST, Special Issue. pp 118-130, Oct 2024
DOI | https://doi.org/10.33411/IJIST/1092
Received | Oct 07, 2024 **Revised |** Oct 13, 2024 **Accepted |** Oct 18, 2024 **Published |** Oct 22, 2024.

Calculating and maintaining trust using Hyperledger Fabric in smart systems plays a vital role in mitigating various trust-related attacks. Current smart systems encounter several challenges, including dependence on centralized trust authorities, which are prone to attacks and present single points of failure, as well as the need to maintain user privacy while establishing trust. Ensuring data integrity and authenticity is equally crucial. In these systems, nodes assess the trustworthiness of other nodes based on their experiences and recommendations. However, trust calculations can be vulnerable to integrity attacks from malicious nodes, such as bad-mouthing and ballot stuffing. To address these threats, trust can be calculated and securely stored on the blockchain. We selected Hyperledger Fabric as the blockchain framework and conducted a prototype implementation of trust calculation on a reduced scale involving 10 nodes. Hyperledger Fabric, being a private, permissioned blockchain, is suitable for decentralized trust calculations and storage in smart devices. We simulated a healthcare scenario within an HLF network, demonstrating secure trust calculation among IoT devices. The results indicate that leveraging the cryptographic properties of blockchain significantly enhances the overall security and trustworthiness of smart systems.

Keywords: IoT Trust, Privacy, Smart Healthcare, Blockchain, Smart Systems.

Introduction:

In recent years, the convergence of advanced technologies has ushered in a new era of interconnectedness and intelligence, giving rise to what is known as "smart systems." These systems span various domains, including healthcare, supply chain, energy, and transportation, leveraging 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 brings significant challenges, with the establishment and preservation of trust in a decentralized and complex environment being among the most critical.

Smart systems face numerous challenges, primarily due to the vulnerabilities of IoT devices, which serve as the weak link in the network. These systems consist of a multitude of sensors and processing devices that exchange vast amounts of data daily. Real-time communication among IoT devices is essential for the functionality of any smart system. However, these devices often come with constraints such as limited storage, low power availability, battery operation, and security/privacy concerns. Ensuring secure data exchange between the various nodes of a smart system is paramount, requiring robust authentication of legitimate users alongside confidentiality, integrity, and privacy of data. Given these limitations, trust in IoT devices within smart systems is often compromised. A single compromised IoT device can pose significant risks, and a smart system that is unaware of such compromises can be highly vulnerable. Trust is foundational to any successful system, influencing user behavior, data sharing, and collaboration. Traditional centralized trust models, where a central authority maintains and arbitrates trust, are frequently inadequate for smart systems, which operate across distributed networks. This necessitates the development of novel mechanisms to ensure trust without relying on a single point of control.

Blockchain technology, along with its cryptographic primitives, emerges as a transformative solution in this context. Initially gaining prominence through its application in cryptocurrencies, blockchain's potential extends far beyond digital currencies, with applications in supply chain transparency, digital identity, secure data sharing, and decentralized applications. At the core of blockchain's functionality are cryptographic primitives that provide security, immutability, and consensus mechanisms. In smart systems, where participants interact autonomously and dynamically, trust becomes a multifaceted concept that includes the authenticity and integrity of data as well as the behavior and intentions of the entities involved. Cryptographic primitives enable the establishment and validation of these dimensions of trust in a decentralized manner, ensuring that smart systems operate reliably and securely.

This paper aims to contribute to the emerging field of trust in smart systems by exploring the synergies between the cryptographic primitives of blockchain technology and smart systems. We propose and implement a comprehensive healthcare system that incorporates on-chain trust calculations, addressing the challenges of trust in dynamic environments.

Objective of Study:

The objective of this study is to utilize blockchain technology for trust calculation, aiming to prevent miscalculations and to safeguard trust values from tampering by malicious nodes.

Novelty Statement:

Adaptive trust has not been previously calculated or stored on the blockchain by any developers or researchers. This paper highlights this novel aspect.

Literature Review:

The literature on trust reveals a significant gap in research related to context-based or adaptive trust, particularly in IoT-based smart systems, vehicular networks, supply chains, data networks, and healthcare systems [9]. While blockchain technology has been effectively utilized to secure transactions and maintain data integrity in these areas (as summarized in Table 1),

mechanisms for trust calculations and adaptive trust are notably lacking [9]. For example, in IoT systems, blockchain may secure terms and obligations but does not assess trust among devices [4]. Similarly, in vehicular networks, while blockchain ensures message integrity, it does not manage trust between communicating vehicles [16][17]. In supply chain and data network smart systems, although blockchain enhances data security and transparency, it does not calculate trust scores for participants or devices [12, 14]. Even in healthcare systems that incorporate fog computing, context-based trust is calculated, but blockchain is not used for trust computation or storage [2]. This lack of adaptive trust mechanisms makes these systems vulnerable to integrity attacks, undermining the overall trustworthiness that is essential for their effective operation and security [7]. Figures 1 and 2 illustrate how blockchain can facilitate the provision of trust and the calculation of trust, respectively.

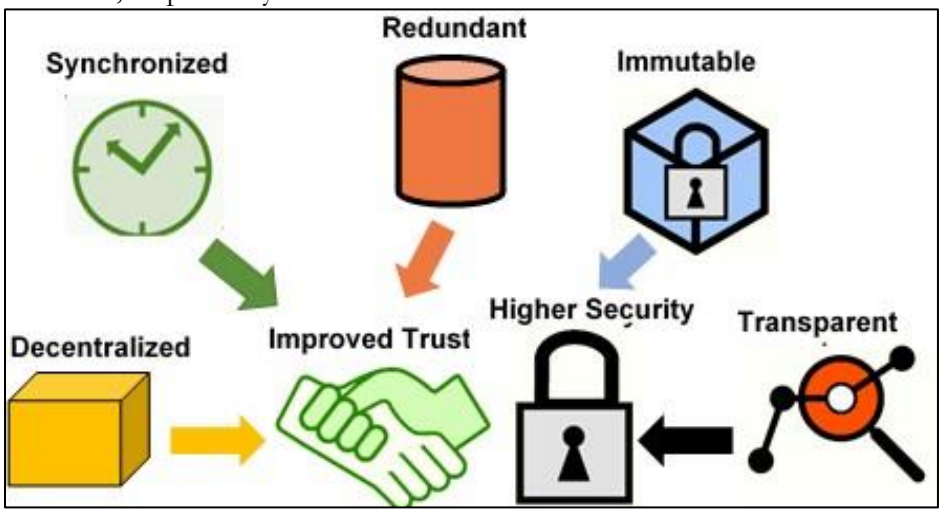


Figure 1. Improving Trust with the Usage of basic primitives of The Blockchain

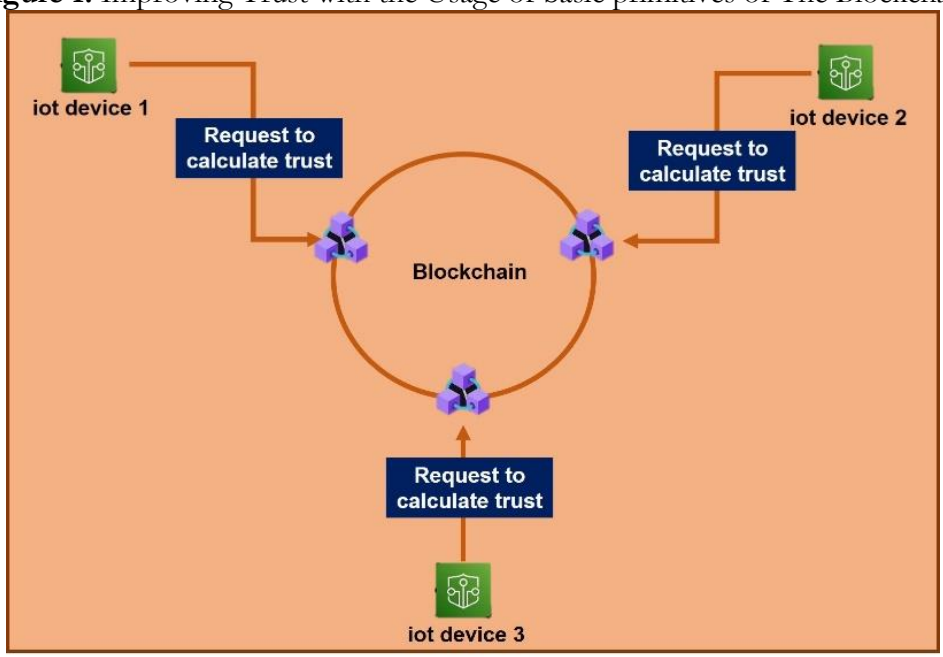


Figure 2. Trust calculation of IoT devices using blockchain.

Proposed Solution and Architecture:

Trust in Healthcare- A Case Study:

Let's consider a case study focused on calculating trust for IoT devices within a healthcare system. This investigation will explore how trust can be assured and managed for

various IoT devices operating in a hospital environment. A private hospital may have implemented an IoT-based healthcare system designed to remotely monitor patients' vital signs and ensure timely medical interventions. This system encompasses a range of IoT devices, including wearable sensors, bedside monitors, and medical imaging equipment. The objective is to calculate and manage the trustworthiness of these IoT devices to ensure the accuracy and security of patient data, thereby enabling informed decision-making by healthcare professionals. We will develop a prototype trust management system that aggregates trust factors for each IoT device and assigns an overall trust score. This score will be displayed to healthcare professionals and administrators, indicating their confidence level in each device's data.

Real-time monitoring and alerting mechanisms can be established to trigger notifications if a device's trust score drops below a predefined threshold. Remediation actions may include temporarily disabling the device, initiating diagnostics, and notifying the IT or biomedical engineering team for further investigation. By leveraging blockchain technology to calculate and manage trust in IoT devices within the healthcare system, hospitals can ensure patient safety, maintain data integrity, and achieve regulatory compliance, ultimately enhancing the overall quality of patient care.

Device Identity and Registration:

Each IoT device is registered on a blockchain network with a unique identity. Smart contracts are deployed to verify the authenticity of these devices, ensuring that only authorized devices can access the network.

Data Collection:

IoT devices transmit selected trust parameter values to the blockchain, where smart contracts are employed to record this data, ensuring its integrity.

Trust calculation and storage:

Trust parameters, including response time, latency, and packet loss ratio, are defined as attributes within the blockchain network. A smart contract will calculate the aggregate trust for each IoT device based on these parameters.

Data Integrity and Immutability:

Blockchain is renowned for its ability to create a tamper-resistant and immutable ledger of transactions. Once trust is calculated and recorded on the blockchain, it becomes exceedingly difficult to alter or tamper with the trust value. This enhances confidence in the accuracy and authenticity of the information.

Decentralization and Security:

Trust values for IoT devices and nodes are calculated centrally. However, by utilizing a decentralized blockchain, reliance on a single point of control is diminished, making it more challenging for malicious actors to compromise the network.

Alerts:

Smart contracts will trigger alerts or notifications when a device's trust score falls below a specified threshold, prompting healthcare staff to take appropriate action. Trust values for IoT devices, whether calculated centrally or decentralized, remain under continuous threat and are vulnerable to integrity attacks if not stored on the blockchain. To mitigate the risk of compromised trust values, blockchain technology can significantly enhance trust calculations and ensure the reliability of IoT devices.

As a result, we are motivated to implement blockchain to calculate and securely store the trust values of legitimate nodes, thereby preventing integrity attacks. Trust values will be computed and saved on the blockchain, reinforcing the overall trustworthiness of the system.

Proposed HLF Architecture:

In a private hospital setting, Hyperledger Fabric is the most suitable type of blockchain for calculating and preserving trust values, as illustrated in Figure 3. This scenario encompasses a hospital featuring an Orthopedic Department, a Cardiology Department, and a Laboratory.

Table 1. Trust management using blockchain

Ref	Specifications					
	Title	**Content Based Trust**	**Trust**	**Year**	**Trust Applied in Smart sys**	**Blockchain Usage For**
[4]	A blockchain-based Trust System for the Internet of Things	No	De-centralized	2019	IoT	Terms and Obligations
[3]	A Trust Architecture for Blockchain in IoT	No	Centralized	2018	IoT	Data Source Reputation and Gate- way reputation
[16]	Blockchain-based Decentralized Trust Management in Vehicular Networks	No	De-centralized	2018	Vehicular system	RSU saving data about road conditions, road congestion or free roads
[6]	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.
[12]	Trust Chain: Trust Management in Blockchain and IoT supported Supply Chains	No	De-centralized	2019	Supply chain system	Interactions among supply chain participants, dynamic trust scores based on these interactions
[1]	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 reduces latency, computational requirements and storage requirements
[14]	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
[13]	Data Trust framework using blockchain technology and adaptive transaction validation	No	De-centralized	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 smart contracts are used for Access, provenance and consent management.
[2]	Early Access context-based adaptive fog computing trust solution for time-critical smart health care systems	Yes	De-centralized	2023	Trust Management in Fog	Blockchain is not used for saving or calculating the trust values.

Channels and CA:

Each department operates its own separate blockchain, referred to as a channel in Hyperledger Fabric (HLF). Each department is assigned a distinct channel, complete with its own Certificate Authority (CA). Any node or peer wishing to interact with the blockchain must be registered and enrolled with the CA of that specific channel. This setup ensures the privacy and confidentiality of departmental data. Nodes or peers that are not registered to a channel are not authorized to access the data within that channel, thereby establishing a robust access control mechanism to mitigate identity-based attacks, such as Sybil attacks. Additionally, the peers within a channel are categorized into different roles, ensuring that no peer can exceed its authorization level.

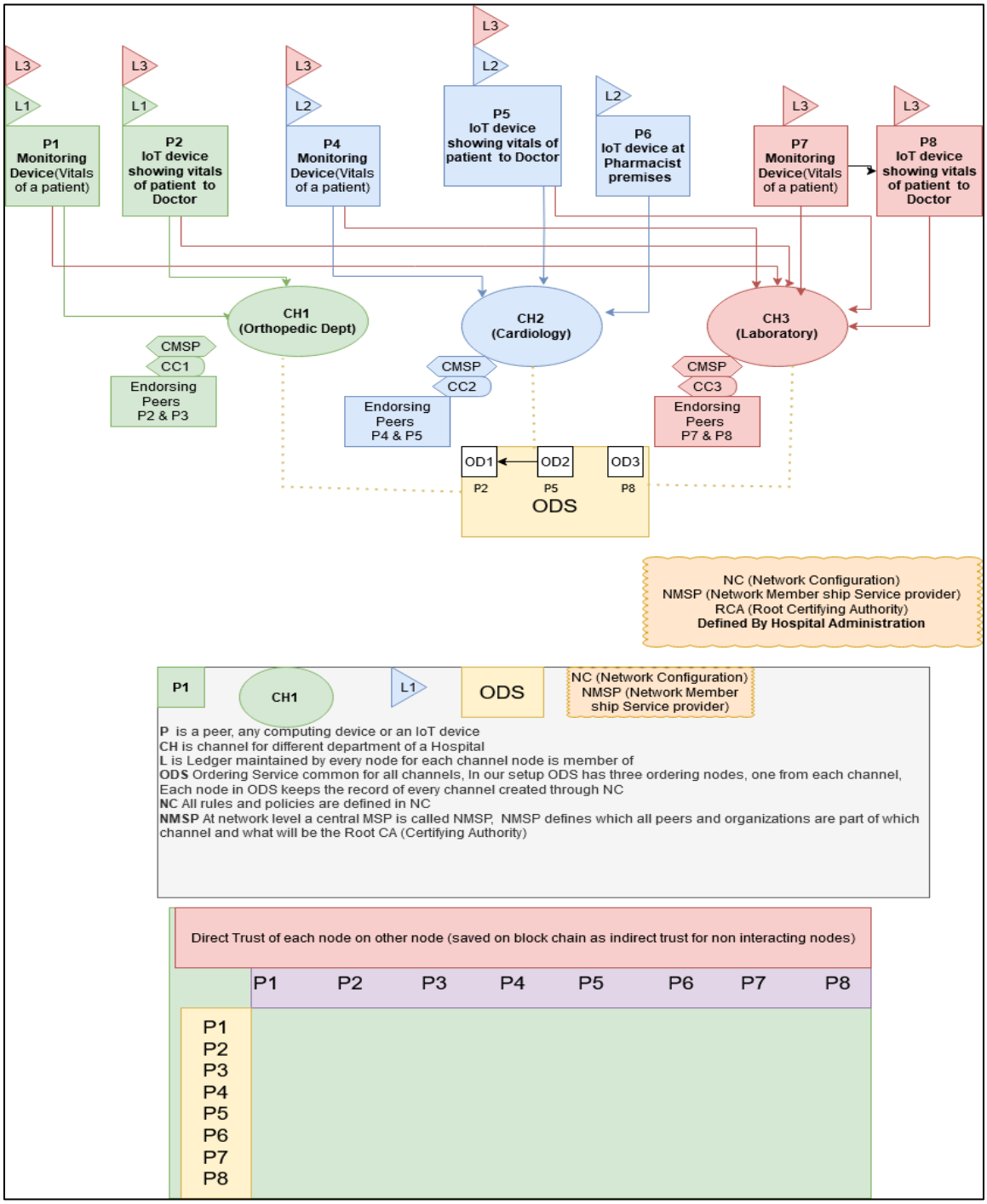


Figure 3. Trust Management using Hyper Ledger Fabric

Endorsing Peers:

These peers are responsible for validating a chain code or smart contract. Endorsing peers execute the chain code and monitor its outcomes. If the results from multiple endorsing peers—based on the number required for agreement defined in the initial configuration—align with expectations, the endorsing peers confirm the legitimacy of the chain code. Subsequently, the code will be deployed and executed on that channel. This process ensures that no malicious code is executed on the blockchain, thereby guaranteeing that only legitimate code runs on the designated channel.

Ordering Peers:

At least one peer in each channel must serve as an ordering peer. Ordering peers are responsible for ensuring the correct sequencing of blocks committed to the channel. Accurate sequencing facilitates easier tracking of the desired blocks.

Committing Peers:

Peers, apart from endorsing and ordering peers, must function as committing peers and must be registered with the channel's Certificate Authority (CA). When a chain code or smart contract is invoked by any committing node, the already endorsed and authorized chain code is executed, producing the required output. The chain code requires certain trust parameter values as input, and the blockchain generates the corresponding trust value as output. This output is then stored on the blockchain. Consequently, blocks containing these transactions are sent to the Ordering and Delivery Service (ODS) for commitment to the blockchain. Once a block is committed and becomes part of the blockchain, it cannot be altered.

Chain Code/Smart Contract:

A chain code and a smart contract refer to the same concept; they are pieces of code created to perform specific tasks. In our scenario, the chain code will be responsible for calculating and storing the trust values of any node whose services are needed.

Proposed Trust Parameters:

The chain code will calculate trust based on the values provided. From a variety of trust parameters, the following proposed parameters will be used as input for the trust calculation.

Response Time:

The time taken to send a request and receive a reply is referred to as response time. A shorter response time typically indicates a higher level of trust in the responder.

Packet Loss Ratio:

The packet loss ratio is defined as the proportion of packets lost during transmission compared to the total number of packets sent. A lower packet loss ratio corresponds to a higher trust value for the sender.

Latency:

Latency refers to the time it takes for a packet to travel between two nodes. Lower latency indicates a higher level of trust in the node sending the packets.

The three values mentioned—response time, packet loss ratio, and latency—will be used as inputs by the smart contract to calculate trust. Since there is no universal formula for trust calculation, we propose using a weighted sum of these input parameters as the calculation method.

$$T = j * k + l * m + n * o \qquad (1)$$

T = Trust value of any node being calculated.

j = Weightage of 1st Trust Parameter, how much part this parameter plays in the calculation of overall trust value;

k = 1st parameter itself i.e. response time.

l = Weightage 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 manner, trust will be calculated using a blockchain smart contract and recorded on the blockchain as direct trust. For instance, the direct trust of node P1 on node P4 will be established. This same value of direct trust will then serve as indirect trust for other nodes, such as P2, P3, P5, and P6.

Discussion and Results:

Limitation of Experimental Setup:

In a real-world system, IoT devices would need to provide trust parameter values to the blockchain for trust calculation after each interaction with other devices. In our scenario, however, the IoT devices are simulated rather than real. We employ a random number generator function to create values for trust parameters—specifically, latency, response time, and packet loss ratio—mimicking the behavior of actual IoT devices. These generated values are then input into the smart contract, allowing the blockchain to calculate the corresponding trust values.

Invoking of Smart Contract:

In this setup, ten IoT devices, each with different locations and types of services, are enrolled with the Certificate Authority (CA) of their respective channels. These devices interact with smart contracts as clients, invoking contracts that have already been endorsed and installed on the blockchain. Each time a device invokes a smart contract, it retrieves the previously stored direct trust value from the blockchain. If no direct trust value exists, the system resorts to the indirect trust value.

This is where adaptive trust comes into play. The blockchain assesses the similarities between the recommenders and the device requesting the trust value. If the location and type of service of the requester align with those of the recommenders, the relevant values are fetched, and the average value of all matching recommenders is calculated as the indirect trust. Total trust is then determined by adding the direct trust and the indirect trust.

In an exceptional scenario where no trust value is available—neither direct nor indirect—a neutral value of 0.5 is assigned to that node for the next interaction, serving as the indirect trust value.

Thresholding of Trust Values:

Once the trust values are retrieved from the blockchain, they become available to the requesting node or IoT device. If the trust value exceeds 0.5, it serves as a green signal for the node to engage with the specific service provider. Conversely, if the value is 0.5 or lower, the requesting node will seek services from other available nodes.

Avoidance of Trust-related Attacks:

Once calculated and stored on the blockchain, the trust values of interacting peers or IoT devices are safeguarded against various threats, significantly reducing the likelihood of modification. The integrity of these values is maintained by blockchain technology, effectively preventing integrity attacks. Features such as immutability, consensus mechanisms, cryptographic security, and transparency work together to create a robust environment resistant to various integrity threats.

In this section, we will evaluate the effectiveness of our implemented architecture and the results achieved following the integration of blockchain technology. Blockchain offers a decentralized and transparent approach to establishing trust across numerous applications, including financial transactions, supply chain management, and voting systems. The key attributes that help mitigate trust-related attacks include immutability, consensus mechanisms, and transparency. Blockchain technology provides a defense against the following types of attacks:

Bad Mouthing Attack:

In a blockchain, the direct trust of interacting nodes is treated as a transaction, which is recorded in blocks linked together through cryptographic hashes. Once a transaction is confirmed and added to the blockchain, it becomes exceedingly difficult to alter or remove it.

This immutability guarantees that false information cannot be retroactively inserted, effectively preventing bad-mouthing attacks.

Ballot Stuffing Attack:

In our implemented system, if a node has not previously interacted with another node, it lacks a direct trust value for that node. Consequently, it will request recommendations from other nodes regarding the specific node in question. In a non-blockchain environment, this is where ballot stuffing attacks can occur, allowing false recommendations from malicious nodes to falsely legitimize them, ultimately undermining the system's overall trust. However, in a blockchain-based recommendation system, each recommendation is recorded as a transaction on the blockchain. Because these transactions are validated through consensus mechanisms, and every participant maintains a copy of the entire ledger, it becomes exceedingly difficult to introduce illegitimate recommendations without detection. The transparency of the blockchain enables all participants to verify the integrity of the recommendation process.

Sybil Attack:

In Hyperledger Fabric, application users must register and enroll with the organization's Certificate Authority (CA). During this enrollment process, users receive the necessary cryptographic materials required for network authentication. Hyperledger Fabric blockchain networks utilize Byzantine Fault Tolerance (BFT) consensus mechanisms to validate transactions, including trust calculations. These consensus mechanisms require participants to demonstrate their commitment to the network, making it costly and resource-intensive to create multiple identities. As a result of these factors, Sybil attacks are effectively prevented in our HLF-based system.

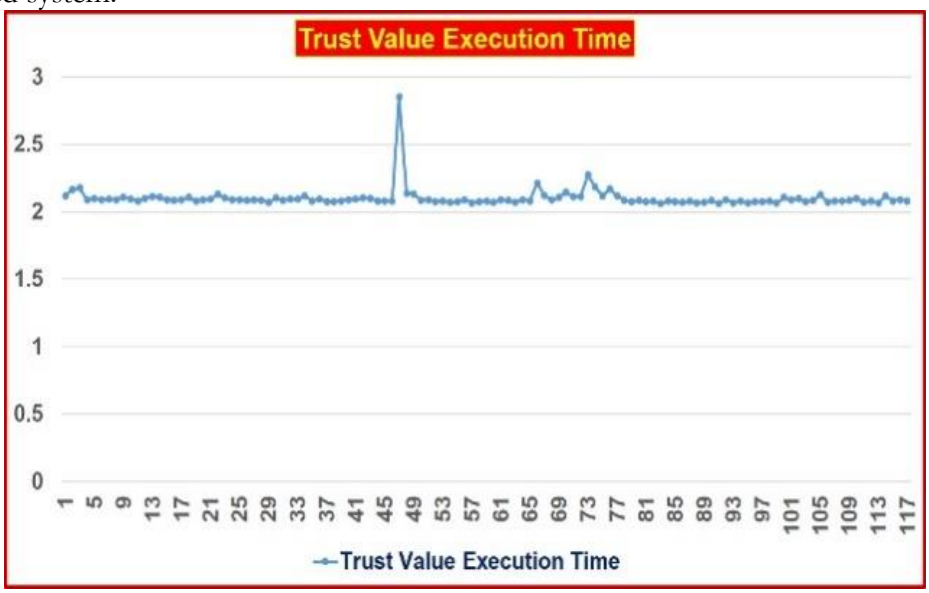


Figure 4. Trust Value Execution Time

On-Off Attack:

On-off attacks occur when participants enter and exit the network at specific times to manipulate the system. In a blockchain network, the consistency of the ledger is upheld through consensus mechanisms. If a participant leaves or joins the network, it impacts their ability to take part in the consensus process, making it more challenging to manipulate the system undetected. Therefore, our HLF-based architecture effectively defends against on-off attacks.

Avoidance of Oracle Problem:

In any blockchain-based system, the oracle problem poses a significant challenge [5]. While blockchain guarantees data preservation once entered, the question arises: what happens if data is modified before being recorded? In our scenario, data is fed to the blockchain in the form of trust parameters such as response time, latency, and packet loss ratio. It is difficult for

an attacker to segregate, interpret, and manipulate this data for malicious purposes. Moreover, even if an attacker were to alter the data, we have a countermeasure in place. By collecting multiple trust parameter values from interacting nodes at different times, we can utilize various parameters for trust calculations, thereby mitigating the oracle problem.

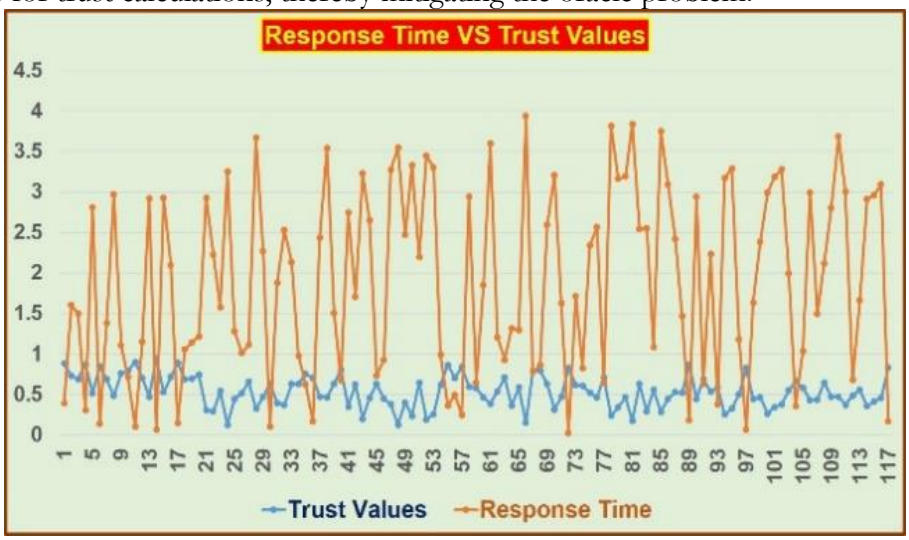


Figure 5. Latency Vs Trust values



Figure 6. Response time Vs Trust values

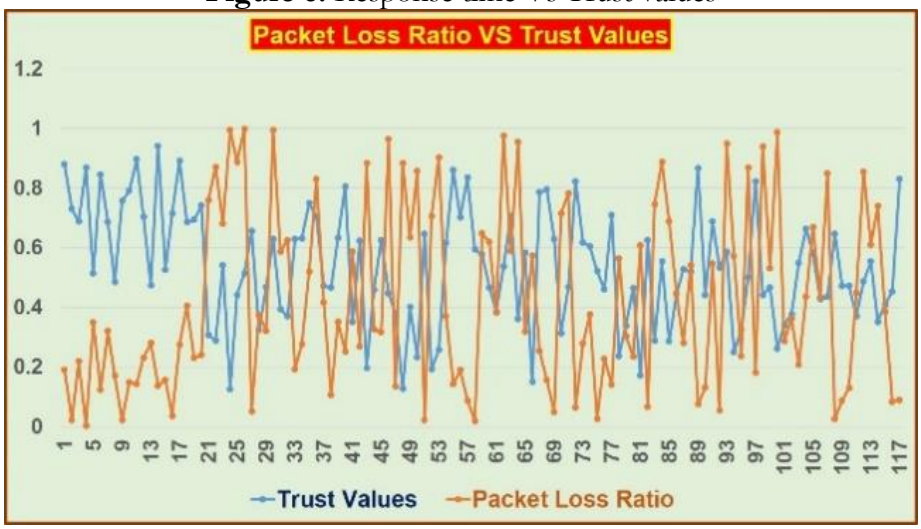


Figure 7. Packet Loss Ratio Vs Trust values

Efficiency of Implemented Solution:

The formulated code was executed over an extended period, during which various parameter values were recorded to evaluate the efficiency of the proposed solution. Data from over 100 transactions was collected, and results were subsequently analyzed.

Trust Value Execution Time:

Another crucial factor in assessing the efficacy of the proposed solution is the time required to obtain a trust value. In a system where hundreds of nodes seek to interact, lengthy wait times for trust values can hinder connections. Analysis of over 100 transactions indicates that Hyperledger Fabric achieves an average response time of no more than 2 seconds. This timeframe is considered optimal for nodes to evaluate trustworthiness and decide whether to establish a connection. Additionally, increasing the processing power of the blockchain's host machine could further reduce this response time. Figure 4 illustrates the data from these transactions.

Latency Vs Trust Values:

The graph illustrating the relationship between latency and trust values clearly demonstrates an inverse correlation between the two parameters. Despite latency contributing only 20 percent to the overall trust calculation, its influence is significant. Specifically, a lower latency results in a higher trust value. Figure 5 depicts this relationship between latency and the calculated trust values.

Table 2. Comparison of existing research to the proposed solution

Ref	Bad Mouthing Attack	Ballot Stuffing Attack	Sybil Attacks	On Off Attacks	New Comer Attacks	Trust Stored Block Chain
[5]	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered
[6]	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered
[18]	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered
[8]	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered
[14]	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered
[1]	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered
[16]	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered
[15]	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered	Not Catered
[4]	Not Catered	**Catered**	**Catered**	Not Catered	Not Catered	Not Catered
[3]	**Catered**	**Catered**	Not Catered	Not Catered	Not Catered	Not Catered
[2]	**Catered**	**Catered**	**Catered**	**Catered**	**Catered**	Not Catered
This Research work	**Catered**	**Catered**	**Catered**	**Catered**	**Catered**	**Catered**

Response Time Vs Trust Values:

Another parameter used in the calculation of trust values is response time. The graph comparing response time to trust values indicates a clear inverse relationship between the two. According to the proposed formula, response time carries a weight of 50 percent in the overall trust calculation. Its impact is evident: lower response times lead to higher trust values. Figure 6 illustrates this relationship between response time and the calculated trust values.

Packet Loss Ratio Vs Trust Value:

The number of packets lost during communication is a critical factor in calculating trust. A higher packet loss ratio results in trust values dropping to zero. This relationship is clearly illustrated in the graph depicting the correlation between packet loss and trust values. Figure 7 presents the relationship between the packet loss ratio and the calculated trust values.

State-of-The-Art-Comparison:

The existing literature on trust reveals that few researchers have focused on context-based or adaptive trust. Notably, no studies have utilized blockchain for the calculation and storage of trust values to mitigate integrity attacks. Consequently, gaps and vulnerabilities persist in the current research on trust within smart systems. Existing studies do not address all potential trust-related attacks. In contrast, our research, which incorporates blockchain technology, comprehensively addresses all possible trust-related attacks, as outlined in Table 2.

Conclusion:

Trust is a fundamental aspect of today's smart world; without it, any smart system would quickly collapse. Context-based trust enhances this foundation, as trust calculated with regard to the specific context proves to be more valuable and enduring. However, the process of calculating context-based trust is vulnerable to integrity attacks from malicious nodes. To mitigate such threats, the total calculated trust is stored on the blockchain, which is immutable and cannot be altered by any malicious actor. Blockchain-based trust is inherently secure against integrity attacks.

Our investigation highlights the crucial role that cryptographic primitives play in strengthening trust within smart systems. By integrating these primitives with the immutability and decentralization of blockchain, we have created a paradigm where trust is established not through centralized intermediaries but through mathematical proofs and distributed consensus.

In our findings, we demonstrate the effectiveness of cryptographic protocols such as digital signatures, hashing, and encryption. These mechanisms are vital for securing communications, authenticating identities, and creating tamper-resistant records that form the bedrock of trust in a decentralized environment. Additionally, our work elucidates the symbiotic relationship between cryptographic primitives and the overarching principles of blockchain, showing how their collaboration can tackle the diverse challenges faced by smart systems. We have validated our approach through concrete implementations and simulations, showcasing both its theoretical potential and practical applicability across various contexts.

Nevertheless, we recognize that our journey is merely a prelude to the expansive challenges that lie ahead. As the landscape of smart systems continues to evolve, so too must our strategies for fostering trust and protecting data. There are significant opportunities for deeper exploration of advanced cryptographic techniques, privacy-enhancing protocols, and innovative consensus mechanisms that could redefine trust and security.

In conclusion, our effort to leverage the cryptographic primitives of blockchain for trust in smart systems has illuminated a path toward a more resilient, transparent, and decentralized future. By combining the power of mathematics with the capabilities of distributed ledgers, we have revealed a landscape where trust emerges from the collaboration of code, computation, and consensus. As we look forward, we are ready to embrace the challenges and discoveries that await us on this dynamic journey of technological advancement and societal transformation.

Author's Contribution: All authors contributed equally

Conflict of Interest: There exists no conflict of interest for publishing this manuscript in IJIST.

References:

[1] Mabrook S Al-Rakhami and Majed Al-Mashari. A blockchain-based trust model for the Internet of Things supply chain management. Sensors, 21(5):1759, 2021.

[2] Aiman Almas, Waseem Iqbal, Ayesha Altaf, Kashif Saleem, Shynar Mussiraliyeva, and Muhammad Wajahat Iqbal. Context-based adaptive fog computing trust solution for time-

critical smart healthcare systems. IEEE Internet of Things Journal, 2023.

[3] Volkan Dedeoglu, Raja Jurdak, Guntur D Putra, Ali Dorri, and Salil S Kanhere. A trust architecture for blockchain in IoT. In Proceedings of the 16th EAI International Conference on Mobile and ubiquitous systems: computing, networking and services, pages 190–199, 2019.

[4] Roberto Di Pietro, Xavier Salleras, Matteo Signorini, and Erez Waisbard. A blockchain-based trust system for the Internet of things. In Proceedings of the 23rd ACM on the symposium on access control models and technologies, pages 77–83, 2018.

[5] Ammar Hassan, Imran Makhdoom, Waseem Iqbal, Awais Ahmad, and Asad Raza. From trust to truth: Advancements in mitigating the blockchain oracle problem. Journal of Network and Computer Applications, 217:103672, 2023.

[6] Youssef Inedjaren, Mohamed Maachaoui, Besma Zeddini, and Jean-Pierre Barbot. Blockchain-based distributed management system for trust in vanet. Vehicular Communications, 30:100350, 2021.

[7] Waseem Iqbal, Haider Abbas, Mahmoud Daneshmand, Bilal Rauf, and Yawar Abbas Bangash. An in-depth analysis of iot security requirements, challenges, and their countermeasures via software-defined security. IEEE Internet of Things Journal, 7(10):10250–10276, 2020.

[8] Firdous Kausar, Fahad M Senan, Hafiz M Asif, and Kaamran Raahemifar. 6g technology and taxonomy of attacks on blockchain technology. Alexandria Engineering Journal, 61(6):4295–4306, 2022.

[9] Rajesh Kumar and Rewa Sharma. Leveraging blockchain for ensuring trust in IoT: A survey. Journal of King Saud University-Computer and Information Sciences, 34(10):8599– 8622, 2022.

[10] Imran Makhdoom, Mehran Abolhasan, Haider Abbas, and Wei Ni. Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125:251–279, 2019.

[11] Imran Makhdoom, Ian Zhou, Mehran Abolhasan, Justin Lipman, and Wei Ni. Privyshare-ing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88:101653, 2020.

[12] Sidra Malik, Volkan Dedeoglu, Salil S Kanhere, and Raja Jurdak. Trust chain: Trust management in blockchain and IoT supported supply chains. In 2019 IEEE International Conference on Blockchain (Blockchain), pages 184–193. IEEE, 2019.

[13] Sara Rouhani and Ralph Deters. Data trust framework using blockchain technology and adaptive transaction validation. IEEE Access, 9:90379–90391, 2021.

[14] Nguyen B Truong, Tai-Won Um, Bo Zhou, and Gyu Myoung Lee. Strengthening the blockchain-based internet of value with trust. In 2018 IEEE international conference on Communications (ICC), pages 1–7. IEEE, 2018.

[15] Liming Wang, Hongqin Zhu, Jiawei Sun, Ran Dai, Qi Ma, and Xin Wei. Trust assessment in Internet of things using blockchain and machine learning. 2020.

[16] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, and Victor CM Leung. Blockchain-based decentralized trust management in vehicular networks. IEEE internet of things journal, 6(2):1495–1505, 2018.

[17] Chenyue Zhang, Wenjia Li, Yuansheng Luo, and Yupeng Hu. Ait: An ai-enabled trust management system for vehicular networks using blockchain technology. IEEE Internet of Things Journal, 8(5):3157–3169, 2020.

Copyright © by authors and 50Sea. This work is licensed under Creative Commons Attribution 4.0 International License.