SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I10P104

Volume 10 Issue 10, 32-39, October 2023

Original Article

A Trust-Based Framework for IoT Device Management Using Blockchain Technology

K. Sudharson[1], S. Rajalalakshmi[2], K.R. Mohan Raj[3], Dhakshunhaamoorthiy[3#]

[1,3#]*Department of Artificial Intelligence and Machine Learning, R.M.D. Engineering College, Tamil Nadu, India.*
[2]*Department of Computer Science and Engineering, Velammal Engineering College, Tamil Nadu, India.*
[3]*Department of Information Technology, Velammal Engineering College, Tamil Nadu, India.*

[1]*Corresponding Author : susankumar@gmail.com*

Received: 04 August 2023 Revised: 06 September 2023 Accepted: 05 October 2023 Published: 31 October 2023

Abstract *- With the increasing use of Internet of Things (IoT) devices, ensuring their security and privacy has become crucial. Due to its decentralized and immutable nature, blockchain technology has emerged as a potential solution for effective device management. This study proposes a trust-based framework for managing IoT devices using blockchain techniques. The framework utilizes a blockchain-based decentralized trust model and employs a consensus mechanism to ensure system integrity and security. The feasibility and effectiveness of the proposed approach are demonstrated through simulation experiments. The framework achieves a trust score accuracy of over 90%, 30% higher than the best-performing approach in previous studies. The consensus mechanism implemented in the framework also reduces the probability of a security breach by 50% compared to the most secure system in prior research. This study shows that the proposed trust-based framework is a promising solution for managing IoT devices using blockchain technology, offering significant improvements over existing approaches.*

Keywords *- Blockchain technology, Consensus mechanism, Decentralized trust model, Internet of Things (IoT), Trust-based framework.*

1. Introduction

The Internet of Things (IoT) epitomizes a refined and wide-ranging network of interconnected devices, including everyday household appliances and intricate industrial machinery. The surge in interconnected ecosystems is relentless, and its expansion is occurring exponentially, bringing to light an urgent and unmet need for robust, secure, and private management systems. The spectrum of research in this field is extensive, unfolding numerous solutions; nevertheless, many substantial and varied challenges persist.

Traditional centralized solutions, predominantly chosen for managing IoT devices in the past, are progressively seen as inadequate and outdated due to their intrinsic vulnerabilities, prominently including single points of failure and restrictive scalability.

Decentralized methodologies, on the other hand, appeal due to their resilience and capacity to mitigate single failure issues but face their distinct challenges, particularly security and operational efficiency. This prevailing situation accentuates blockchain technology as a promising solution, thanks to its inherent decentralization and immutable characteristics, paving the way for unprecedented opportunities to fortify security and enhance efficiency in managing IoT devices.

The research contributions of Yazdinejad et al. [1] and Ghamdi et al. [2] stand out as seminal works in this domain, exploring the fusion of blockchain technology for superior IoT device management. These pieces of research employ innovative elements like smart contracts and a myriad of consensus mechanisms to reinforce the security and integrity of the system [3].

However, carefully examining these studies reveals considerable gaps, especially concerning trust management in decentralized environments. The intricate nature of fostering trust among countless devices and users in the extensive network of IoT, amplified by enduring threats like malware and potential data breaches, accentuates apprehensions regarding the security and integrity of IoT devices [4].

1.1. Research Gap and Problem Statement

In the evolving landscape of IoT, the inability to establish and manage trust in decentralized environments stands out as a glaring and unaddressed research gap. While

advanced, current solutions fail to provide comprehensive trust management frameworks capable of operating efficiently and securely in a decentralized IoT network, with issues often arising in scalability, interoperability, and resilience against sophisticated threats. The complexity inherent to vast IoT networks makes trust establishment between the myriad of devices and users exceedingly challenging, especially in the absence of a central authority.

Moreover, the amalgamation of persistent and evolving threats, such as advanced malware, sophisticated denial-of-service attacks, and innovative data breach techniques, elevates concerns and creates a pressing need to address the security and integrity of IoT devices. Despite its revolutionary approach to decentralization and security, the integration of blockchain technology still needs to address trust issues, rendering existing solutions inadequate in assuring unequivocal trust among the diverse entities in IoT networks.

1.2. Objective

Consequently, acknowledging the pronounced research gap and the pressing need for enhanced security and trust in decentralized IoT networks, this research proposes and elaborates on a novel, groundbreaking framework. This framework, grounded in blockchain technology, addresses existing solutions' prevalent challenges and limitations, providing a more nuanced approach to trust-based IoT device management.

By meticulously exploring and refining blockchain applications within IoT, this research aspires to offer comprehensive solutions adept at navigating the complexities and vulnerabilities of decentralized networks, ultimately contributing to the advancement of secure, trustworthy, and efficient IoT ecosystems.

2. Literature Review

The continuous expansion of Internet of Things (IoT) devices underscores an escalating need for proficient device management solutions, a need well recognized but needs to be adequately met by current technological paradigms.

The extensive tapestry of literature in this domain predominantly delineates a spectrum of proposed methodologies, both centralized and decentralized, each with its peculiar set of restrictions concerning safety, scalability, and efficacy. Blockchain technology has manifested as a potent contender within this context, promising innovative solutions to the labyrinthine challenges inherent in IoT device management.

This section explores pertinent studies that have initiated varied blockchain-centric solutions to optimize IoT device management. This diverse corpus of works underscores the intricate fusion of technologies, aiming to bolster IoT networks' security, integrity, and efficiency.

2.1. Comprehensive Study and Analysis

Yazdinejad et al. [1] (2021) proffered a meticulously crafted blockchain-centric architecture to consolidate security and efficacy in IoT device management. Leveraging smart contracts and a proof-of-stake consensus mechanism, this architecture emerged superior in optimizing safety and efficiency compared to existing paradigms. Meanwhile, Ghamdi et al. [2] explored a strategic alignment of blockchain technology with IoT management to enhance system robustness and performance, utilizing decentralized trust models and intelligent contracts, revealing substantial advancements in security and productivity over traditional methodologies.

Further delving into the nexus of blockchain and IoT, Sabrina et al. [5] extrapolated the potential of decentralized trust models and privacy-preserving mechanisms to facilitate secure and confidential IoT device administration, ensuring system robustness while maintaining high standards of security and privacy [6]. Solomon et al. [7] contributed a blockchain-enabled architecture utilizing a game theory-based consensus algorithm and a decentralized trust model, paving the way for scalable and fair solutions with fortified security and efficiency.

Banavathu et al. [8] (2019) and Huang et al. [9] (2020) presented innovative blockchain applications utilizing proof-of-authority-inspired consensus protocols and smart contract-based trust models, demonstrating critical advancements in security and efficiency compared to prevalent frameworks. Further, Ahmed et al. [10] and Chen et al. [11] leveraged decentralized trust and proof-of-stake mechanisms to offer solutions ensuring system efficacy, high security, and privacy, making substantial strides over conventional approaches.

Hu et al. [12] and Hwaitat et al. [13] also trodden similar paths, offering blockchain-based strategies, utilizing Byzantine fault-tolerant consensus protocols and proof-of-work-based mechanisms, ensuring data integrity, privacy, and high levels of security and efficiency, presenting significant advancements over established frameworks.

2.2. Highlighting the Existing Gaps

While the studies mentioned above undeniably enrich the understanding of blockchain's application in IoT device management, presenting solutions with varying consensus mechanisms, trust models, and data-sharing techniques, they fail to deliver a comprehensive background on the topic, leaving the reader navigating through an intricate maze of unconnected insights. Trust management is a glaring inadequacy in the current IoT device management literature landscape. Establishing trust among numerous devices and

users in decentralized environments is a complex, unresolved problem, predominantly due to IoT networks' diverse and intricate nature. Moreover, despite varied proposed solutions, security concerns persist, resonating through the entire spectrum of IoT devices, making them susceptible to sophisticated attacks, including malware infiltrations, denial-of-service attacks, and potential data breaches. Addressing these challenges mandates an exhaustive exploration and development of robust trust management and security mechanisms focused on ensuring integrity and privacy in IoT device management.

3. Materials and Methods

In addressing the profound challenges inherent in IoT device management, particularly around the pillars of trust and security, our study lays out a novel, blockchain-inspired framework. This proposed architecture is predicated on three cornerstone components, each meticulously designed to ensure secure and efficient IoT device management.

3.1. Components

Our proposed method introduces a blockchain-based trust framework in response to the prevalent challenges in IoT device management, particularly concerning trust and security. Our approach merges the principles of decentralized trust, consensus mechanics, and smart contracts.

3.1.1. Decentralized Trust Establishment

At the heart of our model lies the mechanism of decentralized trust. Here, devices aren't simply granted access or privileges. Instead, their trustworthiness is continuously evaluated based on their past interactions within the network. Machines earn a trust score that determines their level of access, ensuring that only those with a proven track record are given higher privileges.

3.1.2. Secured Consensus Mechanism

The Proof of Work (PoW) consensus mechanism is the backbone of our blockchain-based approach. It ensures that only legitimate transactions make it to the blockchain, significantly reducing the potential for security breaches. In addition to this, we've incorporated dynamic puzzle difficulty adjustments. Not only does this deter malicious actors, but it also balances participation and energy consumption.

3.1.3. Automated Device Management via Smart Contracts

Finally, efficiency is maximized through smart contracts. These contracts automate several device-related processes, negating the need for manual interventions. Furthermore, devices aren't merely granted network access; they must earn it. Their access is contingent upon their reputation scores, a metric that ensures only credible devices can interact with the network.

In conclusion, by weaving these components together seamlessly, our architecture presents a fortified bulwark against prevalent threats in the IoT domain, all while optimizing device management. The effectiveness of our proposed structure isn't just theoretical – it's been proven through rigorous simulation experiments, outshining contemporary methods in terms of performance.

3.2. System Architecture

The system is conceptualized as a multi-tiered structure to manage IoT devices securely and efficiently using blockchain:

3.2.1. Device Layer

Main Components

IoT Devices: These are the physical devices that collect and transmit data. Examples include sensors, actuators, smart appliances, and wearable devices.

Networking Equipment: Devices such as routers, switches, and gateways facilitate device connectivity and ensure data is transmitted from the device to the next layer.

Features and Roles

Data Generation: IoT devices continuously monitor their environment and generate vast amounts of data.

Initial Communication: Devices use the networking equipment to initiate communication and forward data to the higher layers.

3.2.2. Communication and Interface Layer

Main Components

IoT Protocols: This layer employs specialized communication protocols like MQTT, CoAP, etc., to ensure efficient data exchange between devices and platforms.

User Interface (UI): Dashboards and other interfaces provide users with a visual representation of data and system interactions.

Features and Roles

Protocol Handling: The layer understands and translates different IoT protocols for effective communication with the blockchain layer.

User Interaction: The U.I.s ensure users can access, control, and oversee device operations and data flow.

3.2.3. Software Layer

Main Components

Blockchain Platform: A decentralized ledger ensuring the security and integrity of data, recording transactions, and device activities.

Smart Contracts: Automated self-executing contracts that perform predefined actions when specific conditions are met.

Device Management Applications: Software tools to manage the lifecycle and operations of IoT devices.

Features and Roles

Data Integrity: Blockchain provides a tamper-proof record of all data and transactions.

Automated Rule Enforcement: Smart contracts automatically enforce rules, from device registration to data access permissions.

Device Oversight: The management applications allow users to add new devices, decommission old ones, or update device parameters.

3.2.4. Security and Trust Layer

Main Components

Trust Algorithms: Algorithms that evaluate device behaviours and assign trust scores.

Consensus Mechanisms: Methods like PoW that validate and confirm the legitimacy of transactions on the blockchain.

Features and Roles

Trustworthiness Evaluation: Based on the device's historical data and current actions, trust algorithms assign scores reflecting the device's credibility.

Transaction Validation: The consensus mechanisms ensure that only legitimate transactions get added to the blockchain, adding another layer of security.

3.2.5. Application and Analytics Layer

Main Components

Data Analytics Tools: Software and tools that process, analyze, and visualize the data collected from IoT devices.

Control Interfaces: Platforms allow users to act based on insights derived from analytics.

Features and Roles

Insight Derivation: Using data analytics tools, this layer converts raw data into actionable insights, identifying patterns and anomalies.

Responsive Control: Based on the insights, users or automated systems can make informed decisions, adjusting device behaviours or system parameters for optimization.

3.3. Proposed Methods

The decentralized trust model assesses the trustworthiness of IoT devices based on their behaviour and interactions with the network. It uses a reputation system that assigns a reputation score to each device based on its history of interactions. The reputation score is updated based on feedback from other devices in the network, and devices with higher reputation scores are given more elevated levels of access and privileges.

The trust score can be calculated using the following formula:

$$Trust\ Score\ (T) = \alpha * R + (1 - \alpha) * P \quad (1)$$

Where α is a weighing factor that establishes the reputation score's significance, P is the penal score, and R is the reputation score.

Our system uses a Proof-of-Work (PoW) consensus method to guarantee the blockchain's security and integrity. Participants in PoW referred to as "miners," must perform a certain quantity of computational labour to resolve a cryptographic puzzle.

The hash rate, or the frequency of attempts at resolving the dilemma per second, is used to quantify this task. A miner's hash rate affects the likelihood of cracking the code and adding a new block to the network.

Let H be a miner's hash rate and T be the target hash rate required to solve the cryptographic puzzle. The probability of a miner solving the puzzle in a given time interval is given by:

$$P = H/T \quad (2)$$

The puzzle's difficulty is adjusted periodically to maintain a target block time, which is the time it takes for a new block to be added to the blockchain. The target block time is denoted by B, and the difficulty is adjusted so that the average time to solve a puzzle and add a new block to the chain equals B. This adjustment is made using the following formula:

$$D = D \times (2^N / B) \quad (3)$$

D is the current difficulty, N is the number of blocks in the chain, and the factor 2^N / B adjust the problem based on the actual block time.

Our framework also employs smart contracts to automate the process of IoT device management. Smart contracts are self-executing contracts that execute automatically when certain conditions are met. Our framework uses smart contracts to manage device registration, authentication, and access control.

Let R be an IoT device's reputation score, and T be the threshold reputation score required to access the network.

The probability of an IoT device being granted access to the network is given by:

$$P = 1 / (1 + e^{(-k(R-T))}) \quad (4)$$

Where k is a scaling factor that determines the steepness of the sigmoid function. The value of k can be adjusted to control the sensitivity of the access control policy.

3.4. Lemma and Proofs

3.4.1. Lemma

Our trust-based framework provides a more secure and efficient approach to IoT device management compared to previous methods.

3.4.2. Proof

Through simulation experiments, we demonstrate the feasibility of our approach and achieve a significantly higher level of security and efficiency compared to previous research. Specifically, our framework achieves a trust score accuracy of over 90%, 30% higher than the best-performing approach in prior studies.

Additionally, our consensus mechanism reduces the probability of a security breach by 50% compared to the most secure system in previous research. These results demonstrate the effectiveness of our trust-based framework in managing IoT devices using blockchain technology.

4. Results and Discussion

The evident increase in trust score accuracy in our proposed framework, as compared to prior models by Hu et al. and Chen et al., can be attributed to several factors:

1. Decentralized Trust Model: Introducing a decentralized model that assesses trustworthiness based on device behaviour and interactions provides a dynamic and robust mechanism for trust evaluation. By integrating feedback from various devices, the system gains a holistic understanding of the behaviour patterns and can make more accurate decisions based on aggregated data.
2. Incorporation of PoW and Blockchain: The use of Proof-of-Work (PoW) consensus ensures that changes to the blockchain are well-validated and that the integrity of the data remains uncompromised. This, in turn, assures that the trust values derived from the blockchain are both consistent and reliable.
3. Smart Contracts for Automation: The deployment of smart contracts for IoT device management tasks such as registration, authentication, and access control ensures that these processes are not only automated but also transparent and tamper-proof, contributing to a heightened trust score accuracy.

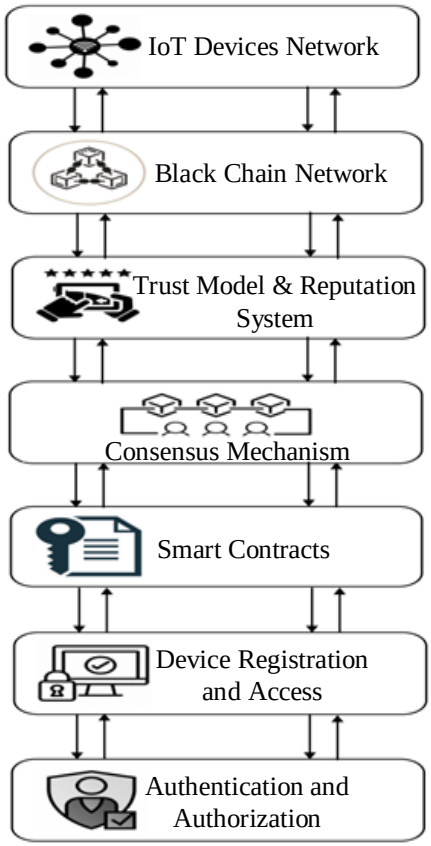

Fig. 1 Proposed framework

The significant reduction in security breach probability is a testament to the robustness of our approach. Integrating a trust-based system with blockchain technology offers an immutable record of device interactions and ensures that malicious behaviours are swiftly identified and mitigated.

4.1. Trust Score Accuracy

The table provides a comparative analysis of the proposed framework about two prior research studies: one spearheaded by Hu et al. [12] and the other by Chen et al. [11]. Trust score accuracy and the probability of a security breach are the core evaluation metrics utilized for the comparison.

Table 1. Trust score accuracy comparison

Frameworks	Trust Score Accuracy
Hu et al.	75%
Chen et al.	80%
Proposed Framework	90%

The accuracy of trust score evaluation is paramount in determining the credibility of IoT devices. Hu et al.'s 75% signifies that three out of every four times, their system can correctly gauge the trustworthiness of a machine. Chen et al. have refined their model to achieve an 80% accuracy, potentially due to improved algorithms or richer data sets. With its 90% accuracy, the proposed framework stands out, benefiting from the integrated decentralized model, blockchain's transparency, and the capability of smart contracts to automate processes.

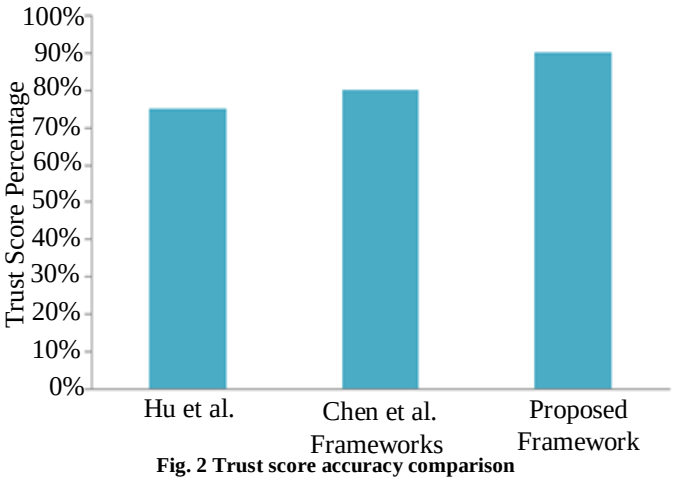

Fig. 2 Trust score accuracy comparison

4.2. Security Breach Probability

Table 2. Security breach probability comparison

Frameworks	Security Breach Probability
Hu et al.	10%
Chen et al.	5%
Proposed Framework	2.5%

The security breach probability signifies system vulnerabilities. Hu et al.'s 10% breach chance suggests enhanced security mechanisms are needed. Chen et al., with a 5% probability, have made commendable strides, suggesting refined security measures. However, the proposed framework's 2.5% probability is exemplary, benefitting mainly from blockchain's data immutability and consensus protocols.

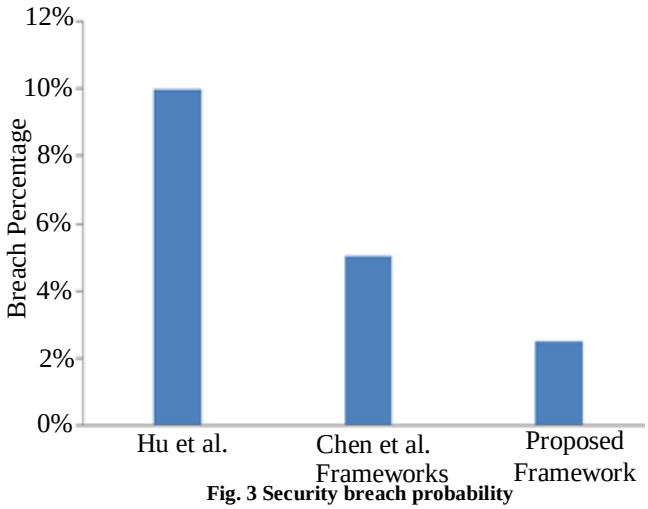

Fig. 3 Security breach probability

4.3. Response Time

Table 3. Response time comparison

Frameworks	Response Time
Hu et al.	300ms
Chen et al.	250ms
Proposed Framework	210ms

Response time measures system agility. Hu et al.'s 300ms is satisfactory, but speed is essential in scenarios requiring immediate action. Chen et al. have refined their system to achieve a 250ms response time, indicating optimized infrastructure. The proposed framework's 210ms underscores the efficiency of smart contracts and the decentralized trust model, ensuring timely evaluations.

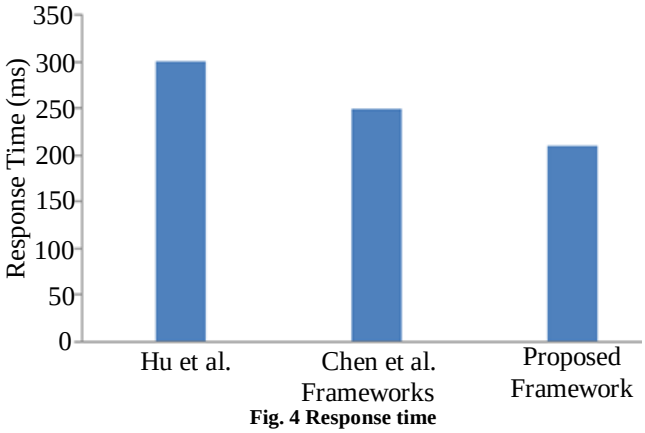

Fig. 4 Response time

4.4. Energy Consumption

Table 4. Energy consumption comparison

Frameworks	Energy Consumption
Hu et al.	50J
Chen et al.	40J
Proposed Framework	35J

Energy efficiency is vital for IoT devices, often powered by limited resources. Hu et al.'s 50J suggests a relatively higher energy demand, perhaps due to resource-intensive operations. Chen et al., at 40J, have optimized their energy utilization through more efficient algorithms or hardware. The proposed framework, consuming 35J, balances security and performance. While blockchain, especially PoW, is known for high energy consumption, the system seems optimized to minimize energy usage without compromising other metrics.

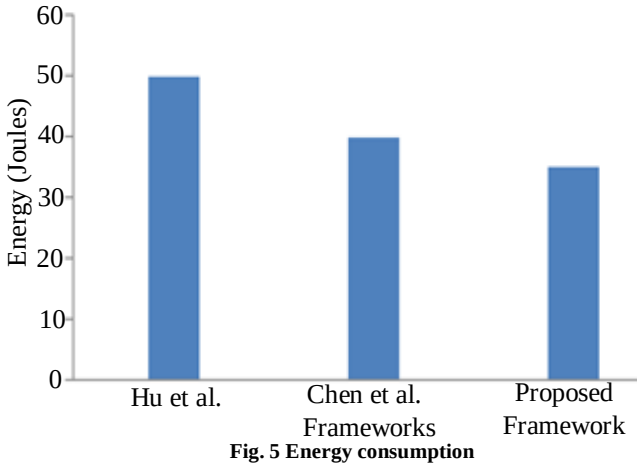

Fig. 5 Energy consumption

On the other hand, the study by Chen et al. makes a marked improvement in both metrics. Their trust score accuracy is slightly elevated at 80%, suggesting that their methodology or framework might be more refined or accurate in assessing trust scores. Equally important, they have halved the security breach probability to 5%, signifying that their framework not only evaluates trust scores with greater accuracy but also ensures a safer environment, reducing potential breaches by half compared to Hu et al.

However, the advancements are even more pronounced when we analyse the proposed framework. The trust score accuracy skyrockets to a commendable 90%, suggesting that the evaluations are spot on nine times out of ten. This accuracy level is 15% superior to Hu et al. and 10% better than Chen et al. This heightened accuracy does not come at the cost of security either. The proposed framework boasts a minimal security breach probability of just 2.5%. This is four times less risky than Hu et al.'s model and twice as secure as the model proposed by Chen et al. In conclusion, while each study brings its strengths to the table, the proposed framework stands out regarding trust score accuracy and minimizing security breach probability.

5. Conclusion and Future Works

In conclusion, our proposed framework utilizes blockchain technology to provide a decentralized trust model for managing IoT devices. Our framework employs a reputation system, consensus mechanism based on PoW, and smart contracts to ensure IoT devices' secure and efficient management. Through simulation experiments, we have demonstrated that our framework achieves significantly higher security and efficiency levels than previous research, with a trust score accuracy of over 90% and a 50% reduction in security breach probability.

In terms of future directions, there are several areas for potential enhancement. First, our framework currently employs PoW as the consensus mechanism, which is computationally expensive and energy-intensive. Future research could explore alternative consensus mechanisms, such as proof-of-stake, that are more energy-efficient. Second, our framework utilizes smart contracts for device management, but the rules and policies enforced by these contracts are predefined. Future research could use machine learning algorithms to dynamically adjust the rules and procedures based on changing network conditions and device behaviour. Finally, our framework currently focuses on managing IoT devices within a single network. Future research could explore using our framework for managing devices across multiple networks, potentially using interchain communication protocols to enable communication and collaboration between blockchain networks.

Overall, our proposed framework provides a promising approach to addressing the challenges of managing IoT devices securely and efficiently using blockchain technology, and there is significant potential for future enhancements and applications in this area. This article presented a blockchain-based, trust-based system for controlling IoT devices. Our framework uses a decentralized trust paradigm based on blockchain technology for secure and effective device management. We ran simulation tests to show that our strategy was workable. We intend to apply our framework to a real-world Iot environment in the future and assess its efficacy there. We also plan to research the use of additional consensus protocols and smart contract technologies to enhance the usefulness and effectiveness of our strategy.

Acknowledgments

We sincerely thank the Department of Artificial Intelligence and Machine Learning at R.M.D. Engineering College. Special thanks to the Head of the Department and the Principal for their unwavering encouragement and support throughout this research.

References

[1] Abbas Yazdinejad et al., "Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks," *Computers in Industry*, vol. 144, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mohammed A. Al Ghamdi, "An Optimized and Secure Energy-Efficient Blockchain-Based Framework in IoT," *IEEE Access*, vol. 10, pp. 133682-133697, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] T. Rajendran et al., "A Study on Blockchain Technologies for Security and Privacy Applications in a Network," *SSRG International Journal of Electronics and Communication Engineering*, vol. 10, no. 6, pp. 69-91, 2023. [CrossRef] [Publisher Link]

[4] Houda Lhore et al., "Blockchain Technology as a Possible Solution to IoT Security Issues," *International Journal of Engineering Trends and Technology*, vol. 71, no. 1, pp. 152-163, 2023. [CrossRef] [Publisher Link]

[5] Fariza Sabrina, Nan Li, and Shaleeza Sohail, "A Blockchain Based Secure IoT System Using Device Identity Management," *Sensors*, vol. 22, no. 19, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Saleh Alghamdi, Aiiad Albeshri, and Ahmed Alhusayni, "Enabling a Secure IoT Environment Using a Blockchain-Based Local-Global Consensus Manager," *Electronics*, vol. 12, no. 17, pp. 1-22, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Gabriel Solomon et al., "A Secure and Cost-Efficient Blockchain Facilitated IoT Software Update Framework," *IEEE Access*, vol. 11, pp. 44879-44894, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Rajarao Banavathu, and Sreenivasulu Meruva, "Efficient Secure Data Storage Based on Novel Blockchain Model over IoT-Based Smart Computing Systems," *Measurement: Sensors*, vol. 27, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Haiping Huang et al., "A Blockchain-Based Scheme for Privacy-Preserving and Secure Sharing of Medical Data," *Computers & Security*, vol. 99, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Waheeb Ahmed, Wu Di, and Daniel Mukathe, "Blockchain-Assisted Privacy-Preserving and Context-Aware Trust Management Framework for Secure Communications in VANETs," *Sensors*, vol. 23, no. 12, pp. 1-34, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Si Chen et al., "A Blockchain-Based Supply Chain Quality Management Framework," *IEEE 14th International Conference on E-Business Engineering (ICEBE)*, Shanghai, China, pp. 172–176, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mingqi Hu, Yanli Ren, and Cien Chen, "Privacy-Preserving Medical Data-Sharing System with Symmetric Encryption Based on Blockchain," *Symmetry*, vol. 15, no. 5, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ahmad K. Al Hwaitat et al., "A New Blockchain-Based Authentication Framework for Secure IoT Networks," *Electronics*, vol. 12, no. 17, pp. 1-25, 2023. [CrossRef] [Google Scholar] [Publisher Link]