LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

SECURING NEXT-GENERATION IOT NETWORKS WITH BLOCKCHAIN-ENABLED DECENTRALIZED TRUST FRAMEWORKS

Ambi Rachel Alex[1*], Dr. Syed Hassan Imam Gardezi[2], Krishnendu P S[3], Aruna P[4], P Showmiya[5]

[1]Lecturer, Electrical and Electronic Engineering Department, College of Engineering, Gulf University, Sanad, Bahrain*
[2]Executive Director and Board Member, Union Investments L.L.C., Ras Al Khaimah, United Arab Emirates, Orcid iD: 0009-0006-6171-1238
[3]Assistant Professor , Department of Cyber Security, Nehru institute of technology,Coimbatore
[4]Assistant Professor, Department of Computer Science Engineering, Nehru Institute of Technology,
[5]Assistant Professor, Department of Cyber Security, Nehru Institute of Technology

ambi.alex@gulfuniversity.edu.bh[1]*
hassanwiz17@hotmail.com[2]
indukrishna.ps@gmail.com[3]
arshnala@gmail.com[4]
nitpshowmiya@nehrucolleges.com[5]

Abstract: The rapid expansion of the Internet of Things (IoT) has led to an unprecedented rise in interconnected devices, generating vast volumes of sensitive data that demand robust security and trust mechanisms. Traditional centralized architectures often struggle to ensure integrity, privacy, and resilience against single points of failure, making them unsuitable for next-generation IoT ecosystems. This paper proposes a blockchain-enabled decentralized trust framework to strengthen the security, transparency, and reliability of IoT networks. By integrating distributed ledger technology with lightweight consensus protocols, the framework establishes immutable device identities, secure data exchange, and automated access control without dependence on centralized authorities. The proposed approach enhances interoperability among heterogeneous IoT devices while minimizing latency and computational overhead. Experimental evaluation and comparative analysis demonstrate that the blockchain-based trust model effectively mitigates common threats such as data tampering, spoofing, and unauthorized access, paving the way for a scalable and trustworthy foundation for future IoT applications.

Keywords: Blockchain, Internet of Things (IoT), Decentralized Trust, Network Security, Data Integrity.

1 Introduction

The Internet of Things (IoT) has emerged as one of the most transformative technologies of the digital era, connecting billions of devices across industries such as healthcare, transportation, manufacturing, and smart cities. These interconnected systems enable real-time monitoring, automation, and data-driven decision-making. However, as the number of connected devices continues to grow, so do the challenges related to data privacy, authentication, and secure communication. Traditional IoT frameworks rely heavily on centralized cloud architectures, which often become bottlenecks in terms of performance and security. This centralized approach exposes IoT ecosystems to risks such as single points of failure, data breaches, and unauthorized manipulation of information.

Blockchain technology offers a promising solution to these limitations by introducing a decentralized and tamper-resistant structure for managing trust among devices. Through its distributed ledger and consensus mechanisms, blockchain eliminates the need for third-party intermediaries, ensuring that data exchanged between IoT devices remains authentic and verifiable. The immutable nature of blockchain records provides traceability and accountability, while smart contracts enable automated

enforcement of security policies and access permissions. These features make blockchain a compelling foundation for the development of next-generation IoT security frameworks that emphasize transparency, reliability, and scalability.

Despite its advantages, integrating blockchain into IoT systems presents certain challenges, including computational constraints of resource-limited devices, latency issues, and network scalability. To address these, researchers are exploring lightweight blockchain architectures and hybrid trust models tailored for IoT environments. This paper focuses on designing a blockchain-enabled decentralized trust framework that enhances data integrity, device authentication, and communication security in IoT networks. The proposed framework aims to establish a secure, transparent, and resilient IoT ecosystem capable of supporting the growing demands of modern digital infrastructures.

2. Security Challenges and Trust Deficiencies in Emerging IoT Networks

The Internet of Things has transformed how devices interact and share information across distributed environments. However, this transformation has also introduced complex security challenges due to the large number of interconnected nodes and the heterogeneity of communication protocols. Many IoT devices operate with limited processing power and memory, making them vulnerable to malicious attacks such as spoofing, data interception, and firmware manipulation. Traditional encryption and authentication mechanisms often fail to protect these resource-constrained systems efficiently. Moreover, the absence of uniform security standards across device manufacturers further complicates the establishment of reliable trust relationships among IoT components.

Centralized architectures, which dominate current IoT ecosystems, pose additional risks. Most IoT networks rely on cloud servers or centralized gateways for identity verification, data storage, and access control. This concentration of control creates a single point of failure that can compromise the entire network if breached. Attackers exploiting such vulnerabilities can gain unauthorized access, modify sensor data, or disrupt communication channels, resulting in serious consequences for applications in healthcare, transportation, or industrial automation. Furthermore, centralized systems often lack transparency and accountability in data management, eroding trust between devices, users, and service providers.

Another critical issue lies in the management of trust among diverse and autonomous IoT devices. In dynamic and large-scale environments, it becomes increasingly difficult to evaluate the credibility of devices that continuously join and leave the network. Existing trust models depend on third-party verification authorities, which may not be scalable or resilient under distributed conditions. To build a secure and dependable IoT ecosystem, it is essential to establish a mechanism that ensures integrity, confidentiality, and authenticity without over-reliance on central entities. This growing need for decentralized and transparent trust mechanisms has led to the exploration of blockchain technology as a potential foundation for securing next-generation IoT networks.

3. Design of a Blockchain-Driven Decentralized Trust Framework for IoT

A blockchain-based decentralized trust framework provides a transformative approach to addressing the inherent vulnerabilities of traditional IoT systems. Instead of depending on a central authority, this framework distributes trust among network

participants through consensus-based validation. Each IoT device acts as a node that records and verifies transactions within a shared ledger, ensuring that no single entity can alter or manipulate data. The use of cryptographic hashing and digital signatures guarantees the immutability and authenticity of every record. By embedding security directly into the communication layer, blockchain enables devices to interact securely, even in environments lacking pre-established trust. This architecture creates a transparent and tamper-proof foundation for secure data exchange among heterogeneous IoT components. The proposed framework integrates several core modules device registration, authentication, access control, and trust evaluation, all powered by blockchain mechanisms. When a device joins the network, its unique identity and credentials are stored on the blockchain, preventing duplication or unauthorized imitation. Smart contracts automate access management by defining rules that govern data sharing, ensuring that only verified devices can initiate or respond to transactions. In addition, reputation scoring or trust computation can be integrated within the ledger to dynamically assess the reliability of devices over time. This continuous assessment process allows the network to identify malicious nodes or abnormal activity patterns without relying on centralized supervision.

Furthermore, the decentralized structure of the blockchain enhances fault tolerance and resilience against single-point failures. Even if one or more nodes are compromised, the distributed consensus ensures the overall integrity of the system. The proposed model also promotes interoperability by allowing different IoT platforms to exchange information securely through a standardized blockchain layer. Lightweight consensus mechanisms such as Proof of Authority (PoA) or Delegated Proof of Stake (DPoS) can be adopted to balance security with energy efficiency, making the framework suitable for resource-constrained IoT devices. Overall, this design establishes a scalable and trustworthy infrastructure capable of sustaining the growing demands of next-generation IoT networks.

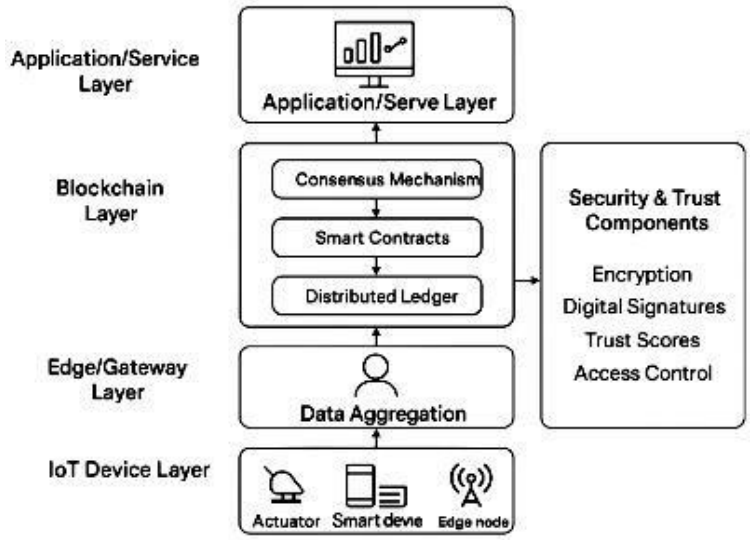

Figure 1. Architecture of the Blockchain-Enabled Decentralized Trust Framework for IoT

Figure 1 illustrates the architecture of the proposed blockchain-enabled decentralized trust framework for IoT. The framework is organized into four functional layers: the IoT Device Layer, Edge/Gateway Layer, Blockchain Layer, and Application/Service Layer. The IoT Device Layer comprises sensors, actuators, and smart devices that generate and transmit data. The Edge/Gateway Layer performs data aggregation,

validation, and lightweight processing before forwarding information to the blockchain. The Blockchain Layer forms the core of the trust mechanism, consisting of a consensus protocol, smart contracts, and a distributed ledger that ensures data integrity and transparency. The Application/Service Layer enables secure data visualization, control, and analytics for end users. Security and trust components such as encryption, digital signatures, trust scoring, and access control span across all layers, ensuring end-to-end protection and decentralized reliability within the IoT ecosystem.

4. Strategic Insights and Future Perspectives for Secure IoT Infrastructures

The integration of blockchain technology into IoT networks represents a fundamental shift in how trust, data integrity, and privacy are maintained in distributed environments. By eliminating centralized control, blockchain ensures that IoT ecosystems become more resilient against tampering, unauthorized access, and data manipulation. This decentralized model not only enhances transparency but also establishes long-term trust among heterogeneous devices and stakeholders. However, its successful deployment depends on aligning blockchain protocols with the resource limitations of IoT devices, where computational capacity and energy consumption remain major concerns. The adoption of lightweight consensus algorithms and adaptive security models will be key to ensuring that the framework remains efficient and scalable. From a broader perspective, blockchain can serve as a backbone for future smart infrastructures that combine IoT with artificial intelligence, edge computing, and 5G communication technologies. These integrations will enable faster, more intelligent, and context-aware decision-making processes at the network edge. Smart contracts can automate device coordination, billing, and access control without human intervention, reducing operational complexity and cost. Additionally, decentralized identity management systems will allow devices to authenticate themselves autonomously, enabling a self-managed, trustless IoT environment. Such advancements will lay the foundation for the next phase of industrial automation, smart cities, and healthcare systems built on secure and transparent data exchange. Moving forward, research efforts should focus on optimizing blockchain performance in large-scale IoT deployments, improving interoperability between diverse blockchain networks, and developing energy-efficient consensus protocols. Collaboration between academia, industry, and policymakers will be essential in establishing standards and frameworks that balance innovation with privacy and security requirements. Ethical considerations, including data ownership and compliance with global privacy regulations, must also be prioritized. In conclusion, blockchain-driven decentralized trust frameworks present a transformative pathway toward building secure, intelligent, and sustainable IoT infrastructures for the connected world of tomorrow.

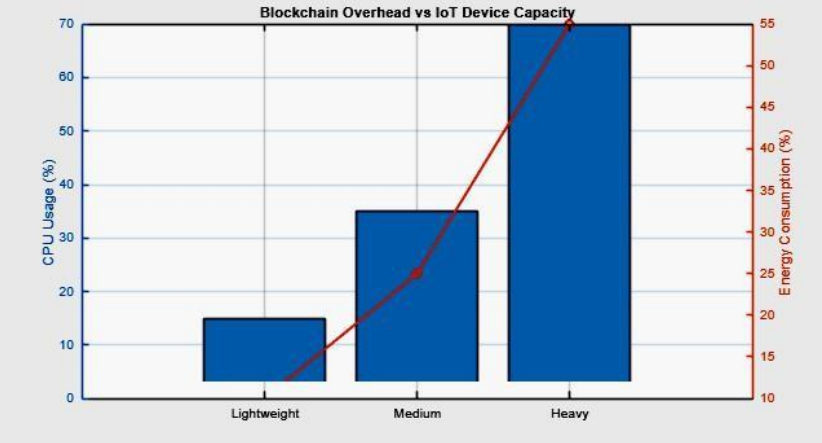

Figure 2. Blockchain Overhead vs. IoT Device Capacity

The simulation result illustrates the relationship between blockchain processing overhead and IoT device capacity. As shown in the plot, lightweight IoT devices exhibit higher relative strain in terms of CPU usage and energy consumption when integrated with blockchain operations, whereas medium and heavy devices handle the computational load more efficiently. This demonstrates that while blockchain enhances data integrity and trust, its implementation must consider the hardware limitations of edge devices. The findings emphasize the importance of developing lightweight blockchain frameworks and optimized consensus mechanisms to achieve a balanced trade-off between security, performance, and energy efficiency in large- scale IoT ecosystems.

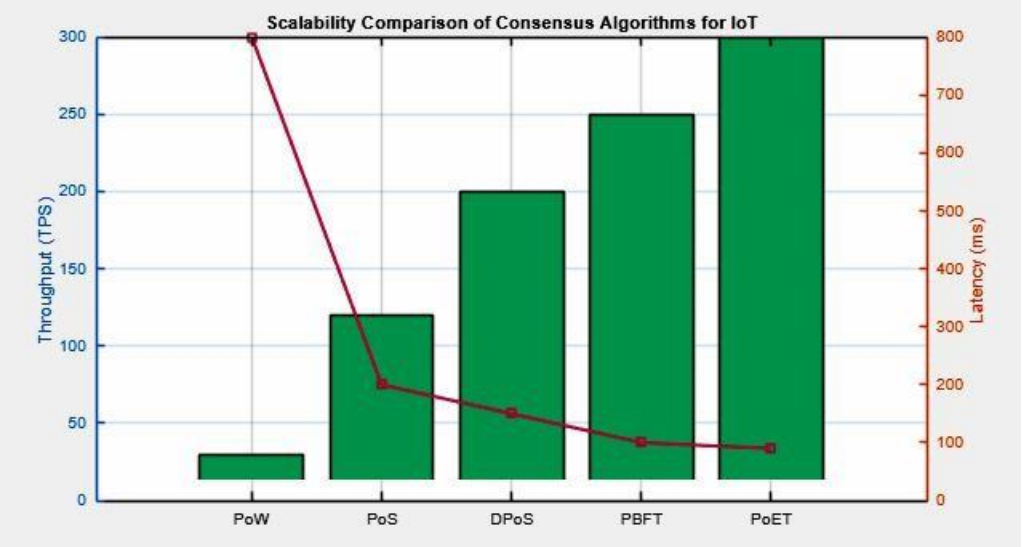

Figure 3. Scalability vs. Consensus Algorithm

The simulation result compares the scalability of various consensus algorithms used in IoT-based blockchain systems by analyzing throughput and latency performance. The plot clearly shows that traditional algorithms like Proof of Work (PoW) offer minimal throughput and higher latency due to intensive computation, making them unsuitable for resource-constrained IoT environments. In contrast, advanced

mechanisms such as PBFT and PoET achieve significantly higher transaction rates and lower latency, indicating better scalability and responsiveness. These results highlight the growing relevance of lightweight and energy-efficient consensus protocols for enabling secure, fast, and scalable IoT infrastructures that can support real-time data exchange and decision-making.

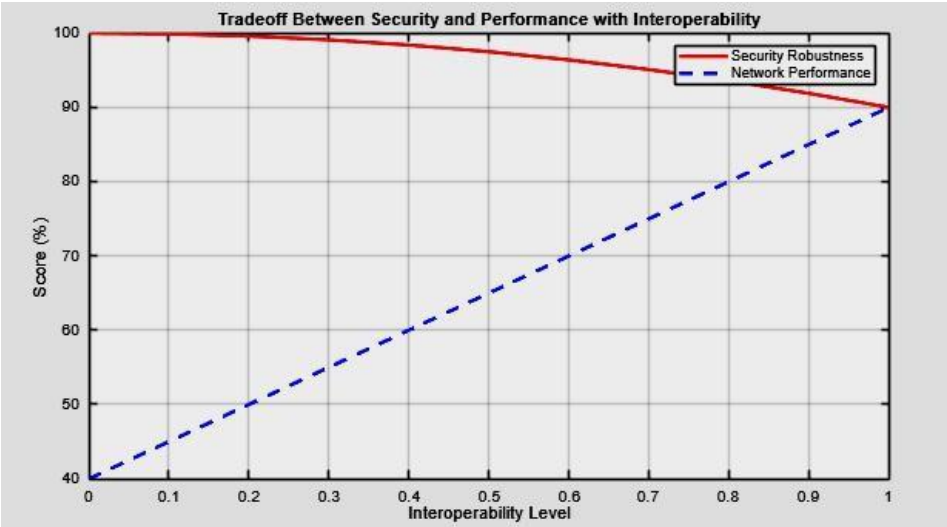

Figure 4. Interoperability Impact on Security and Performance

The simulation result depicts the trade-off between security robustness and network performance as interoperability among IoT systems increases. The plot indicates that higher interoperability enhances overall system performance by improving data exchange and coordination between heterogeneous devices. However, this improvement comes with a slight reduction in security strength, as more open and interconnected systems may expose additional attack surfaces. The analysis emphasizes the need for adaptive security models that can maintain strong protection without compromising efficiency, ensuring that future IoT networks achieve an optimal balance between connectivity, performance, and resilience.

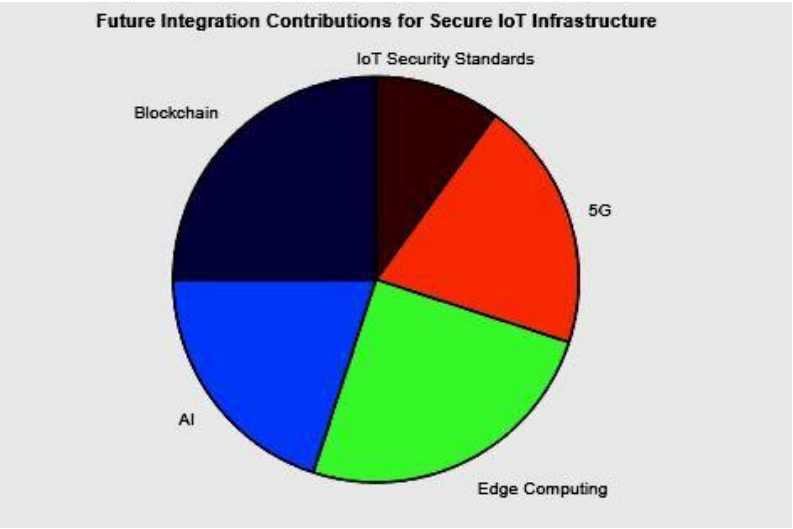

Figure 5. Future Trends – Blockchain Integration with AI, Edge, and 5G

The simulation result highlights the projected contribution of emerging technologies toward the development of secure IoT infrastructures. The pie chart demonstrates that blockchain and edge computing play the most significant roles, each contributing around one-fourth to the overall framework by ensuring data integrity, decentralization, and real-time processing. Artificial intelligence and 5G technologies also provide substantial support through intelligent automation and high-speed connectivity, enabling faster and more reliable device communication. Meanwhile, IoT security standards form the foundational layer that governs data protection and regulatory compliance. Together, these technologies represent a balanced and collaborative ecosystem driving the evolution of intelligent, resilient, and future-ready IoT environments.

5. Conclusion

The expansion of the Internet of Things has created a network where billions of devices share information and perform automated actions in real time. Ensuring security and trust within such a vast and diverse system has become one of the most pressing challenges in modern technology. This paper presented a decentralized trust framework based on blockchain to provide stronger protection for IoT communication and data exchange. By using distributed records and verified transactions, the proposed framework reduces the risks of data loss, manipulation, and unauthorized access that often arise in centralized systems. It also supports transparent and reliable interactions between devices without depending on a single controlling authority.

The proposed design emphasizes secure data sharing, identity verification, and continuous monitoring of device behavior through smart contracts and cryptographic validation. This approach allows the IoT environment to maintain integrity and accountability even when operating across multiple domains and networks. While issues such as scalability and energy usage still require careful consideration, the concept demonstrates that blockchain can serve as a trusted foundation for next generation IoT infrastructures.

In conclusion, a blockchain based trust model provides a clear path toward building safer, transparent, and more dependable IoT systems. It replaces traditional trust mechanisms with a collaborative process that enhances resilience and reliability across all layers of communication. With continued refinement and standardization, such a framework can help shape a secure digital ecosystem that supports the growth of intelligent and connected technologies worldwide.

References

1. “A trusted IoT data sharing method based on secure multi-party computation,” *Journal of Cloud Computing*, vol. 13, article 138, Sep. 2024.
2. Ghayth AL Mahadin, “Leveraging Blockchain Technology for Robust Security and Privacy in Internet of Things (IoT) Systems: Challenges and Solutions,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, issue 22s, 2024.
3. “Standard for Blockchain-Based Zero-Trust Framework for the Internet of Things (IoT),” IEEE Standard IEEE 3219-2023.
4. “Proof-of-resource: A resource-efficient consensus mechanism for IoT devices in blockchain networks,” EAI Endorsed Transactions on Internet of Things, 2024.
5. “Data Privacy and Security Enhancement in Internet of Things Network using Blockchain,” *IEEE Future Networks World Forum (FNWF 2024)*.

6. "Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions," *Applied Sciences*, 2025.
7. "Enhancing Data Trustworthiness in IoT Applications through a Decentralized Blockchain-based Trust Framework," *Journal of Information and Technology*, Vol. 5, No. 6, 2025.
8. "Blockchain Technology for IoT Security and Trust: A Comprehensive SLR," *Sustainability*, vol. 16, no. 23, 2024.
9. IoT Access Control Model Based on Blockchain and Trusted Execution Environment, W. Jiang, E. Li, W. Zhou, Y. Yang, T. Luo, *Processes*, Vol. 11, No. 3, 2023.
10. IEEE standard IEEE 3220.01-2025, "Approved Draft Standard for Consensus Framework for Blockchain Systems."
11. Manpreet Kaur and Shikha Gupta, "Performance Evaluation of A Lightweight Consensus Protocol for Blockchain IoT Networks," *Computer Science*, vol. 26, no. 1, 2025.
12. V. V. S. Sasank, A. Verma, D. Dhabliya et al., "Decentralized and Trustworthy Connectivity in IoT through Blockchain-Enabled Secure Data Sharing over Wireless Networks," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 21s, pp. 274-282, 2024.
13. "zk-IoT: Securing the Internet of Things with Zero-Knowledge Proofs on Blockchain Platforms," G. Ramezan and E. Meamari, arXiv preprint, Feb. 2024.
14. "Fusion Chain: A Decentralized Lightweight Blockchain for IoT Security and Privacy," *Electronics*, MDPI, 2021 (with relevance to lightweight blockchain and PBFT etc.)
15. "A systematic literature review of blockchain technology and energy efficiency based on consensus mechanisms, architectural innovations, and sustainable solutions," *Discover Analytics*, vol. 3, article 14, Sept. 2025.
16. Kaur, Mittal, Jain et al., "Blockchain-enhanced security and Bayesian trust assessment for secure task scheduling in latency-critical fog computing environments," *Journal of Cloud Computing*, vol. 14, article 53, 2025.
17. Mahmoud Abbasi, Javier Prieto, Marta Plaza-Hernandez, Juan Manuel Corchado, "Proof-of-resource: A resource-efficient consensus mechanism for IoT devices in blockchain networks," *EAI Endorsed Transactions on Internet of Things*, vol. 10, Jul. 2024.
18. Abdulrahman Alreshidi, "A framework for blockchain-based management of IoT-driven data sharing," *International Journal of Advanced and Applied Sciences*, vol. 12, no. 1, pp. 208-219, Jan. 2025.
19. Ababio I. B., Bieniek J., Rahouti M., Hayajneh T., Aledhari M., Verma D. C., Chehri A., "A Blockchain-Assisted Federated Learning Framework for Secure and Self-Optimizing Digital Twins in Industrial IoT," *Future Internet*, vol. 17, no. 1, article 13, 2025.
20. QuA. Arshad, W. Z. Khan, F. Azam, et al., "Blockchain-based decentralized trust management in IoT: systems, requirements and challenges," *Complex & Intelligent Systems*, vol. 9, pp. 6155-6176, 2023.
21. S. Addula, "A Novel Permissioned Blockchain Approach for Scalable and Privacy-Preserving IoT Authentication," *JCSRA (The Stap)*, vol. 2025, no. 4, 2025.
22. Jyoti G., "Blockchain-Based Security Framework for Internet of Things in Smart Cities," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 22s, June 2024.
23. Titiya, Mahesh D., "Building Trust on the IoT Connected World: Addressing Security Challenges in IoT Architectures and Applications," *International Journal of*

Intelligent Systems and Applications in Engineering, vol. 12, no. 4, pp. 750-…, 2024.
24. "TBDD: A New Trust-based, DRL-driven Framework for Blockchain Sharding in IoT," Zixu Zhang, Guangsheng Yu, Caijun Sun, Xu Wang, Ying Wang, Ming Zhang, Wei Ni, Ren Ping Liu, Andrew Reeves, Nektarios Georgalas, arXiv preprint, Jan. 2024.
25. Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things, Kai Li et al., arXiv preprint, May 2025.