International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Decentralized Trust in the Internet of Things.

A Comprehensive Survey of Blockchain-Enabled Security Frameworks and Future Directions

Miss Neha Ashok Farande
Department of computer science
Dr. D. Y. Patil Arts, Commerce & Science College.
Email: nehafarande2003@gmail.com

Miss Rutuja Kishor Gosavi
Department of computer science
Dr. D. Y. Patil Arts, Commerce & Science College.
Email: rutujagosavi2003@gmail.com

Abstract

The Internet of Things (IoT) is a cornerstone of digital transformation, yet its centralized architecture remains a primary target for cyber-attacks. This paper systematically evaluates the integration of blockchain technology as a solution to critical IoT vulnerabilities, including identity spoofing, data manipulation, and single points of failure. We analyze a multi-layered taxonomy of IoT threats and evaluate blockchain-based countermeasures such as decentralized authentication, smart-contract-driven access control, and cryptographic privacy preservation. While blockchain offers immutability and transparency, significant barriers remain regarding scalability, energy consumption, and regulatory compliance (e.g., GDPR). This study identifies key research gaps and proposes a roadmap toward lightweight, edge-integrated, and quantum-resistant blockchain architectures for secure IoT ecosystems.

Keywords: Internet of Things; Blockchain; IoT Security; Smart Contracts; Distributed Ledger Technology; Privacy Preservation.

1. Introduction

The exponential growth of the Internet of Things (IoT) has facilitated seamless data exchange across healthcare, industrial, and urban environments. However, the inherent heterogeneity and resource-constrained nature of IoT devices present significant security challenges. Traditional security models, which rely on centralized servers, create bottlenecks and are susceptible to Distributed Denial of Service (DDoS) attacks.

Blockchain technology offers a decentralized alternative. By utilizing a distributed ledger maintained through

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

consensus mechanisms, blockchain provides a tamper-resistant environment suitable for the dynamic nature of IoT. This paper explores the synergy between these two technologies, assessing how decentralized ledgers can redefine data integrity and device trust.

2. Blockchain-Enabled Security Mechanisms

2.1 Data Integrity and Non-Repudiation

In a Blockchain-IoT (BIoT) ecosystem, data integrity is maintained through cryptographic hashing. Every transaction is signed with a private key (e.g., using ECDSA), ensuring that data originates from a verified source.

- **Proof of Trust (PoT):** Used for multi-tier verification.
- **Immutability:** Once a hash is recorded on the ledger, the data becomes computationally impractical to alter.

2.2 Authentication and Access Control

Traditional PKI (Public Key Infrastructure) is difficult to scale for billions of devices. Blockchain facilitates:

- **Genesis Transactions:** Storing initial device identities on the chain for permanent reference.
- **Bubble of Trust:** A decentralized identification method where devices authenticate via tickets and object IDs, eliminating central authority bottlenecks.

2.3 Availability and DDoS Resilience

By distributing the ledger across a peer-to-peer (P2P) network, the "Single Point of Failure" is removed. For an attacker to take down the system, they would need to compromise a majority of the network nodes simultaneously, making standard DDoS attacks infeasible.

3. Threat Landscape and Countermeasures

The current BIoT threat landscape can be

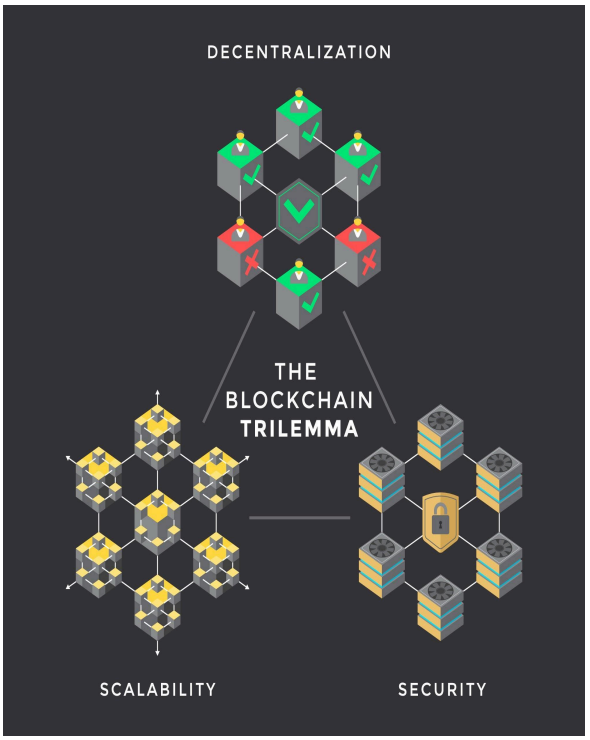
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

categorized into five primary vectors:

4. Current Challenges and Research Gaps

Despite its potential, the integration of blockchain and IoT faces several "hard" technical barriers:

1. **Scalability vs. Decentralization:** Public blockchains like Ethereum struggle with the high transaction throughput required by IoT.
2. **Resource Constraints:** IoT devices often lack the CPU and RAM to perform complex consensus tasks (e.g., mining).
3. **The "Right to be Forgotten":** Blockchain's immutability contradicts GDPR requirements, which mandate the ability to delete personal data.
4. **Energy Consumption:** Proof-of-Work (PoW) is unsustainable for battery-powered sensors.



5. Methods

This study employs a Qualitative-Comparative Research Design.

- **Literature Synthesis:** Analysis of peer-reviewed journals (IEEE, ACM) from 2017–2025.
- **Taxonomy Framework:** Classification of attacks and the mapping of specific cryptographic protocols to those threats.
- **Trend Analysis:** Evaluating the shift from heavy public chains to lightweight consortium/permissioned chains in industrial settings.

6. Findings

- **Decentralization:** Effectively removes single points of failure but increases network latency.
- **Smart Contracts:** These are highly effective for automating security policies but introduce

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

"Code-is-Law" vulnerabilities if the contract itself has bugs.

- **Lightweight Architectures:** The most successful BIoT implementations utilize Edge Computing where heavy blockchain processing is offloaded to local gateways rather than the end-sensors.
- **Privacy:** Standard blockchain is pseudonymous, not anonymous. Advanced techniques like Zero-Knowledge Proofs (ZKP) or Ring Signatures are necessary for true privacy but increase computational overhead.

7. Conclusion

Blockchain is not a "silver bullet" for IoT security, but it is a foundational shift toward a more resilient architecture. To move from prototypes to global deployment, future research must prioritize lightweight consensus algorithms and GDPR-compliant "erasable" pointers. Integrating blockchain with Edge Computing and AI will likely provide the necessary balance between security, speed, and energy efficiency.

Acknowledgment

The authors sincerely thank the faculty of the Department of Computer Science, Dr. D. Y. Patil ACS College, Pimpri Chinchwad, for their guidance and support throughout this research work. We are especially grateful to our project guide for valuable suggestions and encouragement, which greatly contributed to the successful completion of this paper.

References

[1] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and solutions,” IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1731–1754, 2017.

[2] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT: Challenges and opportunities,” Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.

[3] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, “Blockchain’s adoption in IoT: The challenges and a way forward,” Journal of Network and Computer Applications, vol. 125, pp. 251–279, 2019.

[4] J. Lin, Z. Shen, A. Zhang, and Y. Chai, “Blockchain and IoT based food traceability for smart agriculture,” in Proc. IEEE Int. Conf. on Information Systems (ICIS), 2017, pp. 1–6.