IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

Security Challenges in Connected Device Networks: A Blockchain-Based Approach

Vasigala Priyanka[1] and Pinniboina Prasanna Kumar[2]
Lecturer, Computer Science[1]
B.Sc. Computer Science[2]
Sir. C. R. Reddy College of Engineering, Eluru

Abstract: *The rapid expansion of the Internet of Things (IoT) has revolutionized how devices collect, exchange, and process data across a wide range of applications. However, the highly distributed and resource-constrained nature of IoT systems presents significant security challenges, particularly in data integrity, device authentication, and network resilience. Traditional centralized security models, while effective in controlled IT environments, often fail to scale securely in IoT ecosystems due to single points of failure and insufficient auditability. This study explores the integration of blockchain technology into IoT networks as a decentralized solution to address these security vulnerabilities. Through a mixed-methods research design involving both simulation-based experiments and statistical analysis, the paper evaluates blockchain's impact on unauthorized access prevention, tamper resistance, energy efficiency, and latency. A private Ethereum test network was implemented, with smart contracts deployed to automate authentication and access control. Results demonstrate that blockchain significantly reduces unauthorized access attempts and prevents data tampering, with a slight trade-off in latency and energy consumption. A Chi-Square test confirmed the statistical significance of reduced breaches in the blockchain model ($\chi^2(1) = 5.26$, $p = 0.021$). While performance overhead was observed, it remained within acceptable limits for non-critical applications. The findings affirm blockchain's potential as a transformative security layer for IoT environments, especially when data integrity, traceability, and decentralized trust are required. Future research is suggested to enhance scalability, reduce resource demands, and integrate AI for intelligent threat detection in blockchain-enabled IoT systems.*

Keywords: Internet of Things (IoT), Blockchain, IoT Security, Decentralized Networks, Ethereum, Secure IoT Architecture, IoT Authentication

DOI: 10.48175/IJARSCT-28539