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 4, November 2025
Impact Factor: 7.67

An Approach to Identify the Security of IoT Devices: Challenges and Solution

Rachidatou Fofana, Fatou A Bah, Khushboo Tripathi
Sharda School of Computer Science and Engineering, Sharda University, Greater Noida, UP, India

Abstract: *The rapid proliferation of Internet of Things (IoT) devices has revolutionized sectors ranging from healthcare and manufacturing to smart homes and cities. However, this expansion introduces significant security vulnerabilities due to the diverse and often resource-constrained nature of IoT devices. Key challenges include weak authentication mechanisms, lack of standardization, insufficient firmware updates, and susceptibility to physical tampering and cyber-attacks such as DDoS, data breaches, and botnets. To address these challenges, various solutions have emerged, including lightweight cryptography, blockchain-based security models, zero-trust architectures, and AI-driven threat detection systems. Moreover, regulatory frameworks and industry standards are evolving to promote security-by-design principles. Emerging trends indicate a shift toward edge computing for real-time threat mitigation, integration of machine learning for anomaly detection, and the adoption of decentralized identity management systems. Ensuring robust IoT security requires a multi-layered, adaptive approach that balances performance, cost, and scalability across heterogeneous devices and networks. Emerging trends indicate a shift toward edge and fog computing, which helps reduce latency and enhances localized security analytics, minimizing the risk associated with centralized vulnerabilities. The adoption of Zero Trust Architecture (ZTA) is on the rise, enforcing detailed access control measures. Additionally, federated learning is facilitating collaborative AI training without revealing raw data. Furthermore, advancements in post-quantum cryptography aim to protect IoT devices against potential threats posed by quantum computing. As the IoT landscape continues to evolve, ensuring end-to-end security presents a dynamic and complex challenge. A combination of robust design principles, adaptive security frameworks, cross-industry collaboration, and continuous innovation is essential to safeguarding IoT environments and securing their full potential.*

DOI: 10.48175/IJARSCT-29959