

Research on security for IoT devices and building a solution for selecting encryption techniques

Tong Van Truong

Abstract: This study investigates security challenges in Internet of Things (IoT) environments and proposes a framework for the dynamic selection of optimal encryption techniques. IoT devices are inherently constrained by limited computational power, memory, and energy resources, making traditional cryptographic solutions often impractical. The research systematically analyzes common threat vectors, including data interception, device spoofing, and denial-of-service attacks, and evaluates the performance of symmetric, asymmetric, and lightweight encryption algorithms under resource constraints. A multi-criteria decision-making model is developed to select the most suitable encryption technique based on real-time device parameters such as battery level, processing load, and data sensitivity. Experimental results demonstrate that the proposed solution significantly reduces energy consumption and latency while maintaining robust security levels compared to static encryption approaches. The framework offers a scalable and adaptive security mechanism for heterogeneous IoT networks, contributing to enhanced data integrity and confidentiality. This work provides a practical foundation for implementing context-aware cryptographic strategies in smart home, healthcare, and industrial IoT applications.

Keywords: IoT security, encryption techniques, cryptographic selection, IoT device protection