RADemics

Secure Boot and Key Management Protocols for IoT Edge Devices

Nabeena Ameen, R. Rajagopal
B. S. ABDUR RAHMAN CRESCENT INSTITUTE OF SCIENCE AND TECHNOLOGY, ALLIANCE COLLEGE OF ENGINEERING AND DESIGN

Secure Boot and Key Management Protocols for IoT Edge Devices

[1]Nabeena Ameen, Assistant professor (sel gr), Information Technology, B. S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamilnadu, India. nabeena@crescent.educationv

[2]R. Rajagopal, Associate Professor, Department of Computer Science and Engineering, Alliance College of Engineering and Design, Alliance University, Bengaluru, Karnataka, India. rajagopalrmail@gmail.com

Abstract

The proliferation of Internet of Things (IoT) edge devices in critical infrastructure has introduced unprecedented security challenges, particularly in the domains of secure boot and cryptographic key management. Traditional centralized approaches to trust establishment are ill-suited for resource-constrained environments characterized by intermittent connectivity, minimal computational capacity, and vulnerability to physical and remote attacks. This chapter explores lightweight secure boot mechanisms and decentralized key management protocols tailored for IoT edge ecosystems, with a focus on architectural resilience, cryptographic efficiency, and quantum-era readiness. Attack surfaces targeting bootloaders and firmware are critically examined to highlight vulnerabilities exploited during device initialization. Case studies of minimalist bootloader implementations are presented to illustrate practical design constraints and optimizations. The comparative analysis of pre-shared keys, elliptic curve cryptography, and post-quantum cryptographic primitives underscores the trade-offs between security strength, implementation complexity, and energy consumption. Emphasis was placed on lightweight consensus mechanisms for decentralized trust validation and scalable identity management, the feasibility of integrating post-quantum cryptography into ultra-constrained edge devices was assessed, considering performance, memory, and interoperability challenges.

Keywords: Secure Boot, Key Management, IoT Edge Devices, Post-Quantum Cryptography, Lightweight Consensus, Decentralized Security

Introduction

The growing reliance on Internet of Things (IoT) edge devices across critical applications—from industrial control systems to smart cities—has significantly raised the stakes for embedded device security [1]. These devices, often deployed in uncontrolled environments, face elevated risk from both physical tampering and sophisticated cyberattacks [2]. Unlike traditional computing platforms, IoT edge devices are typically built with limited computational resources and minimalistic hardware, making them highly susceptible to attacks during the early stages of system boot and cryptographic initialization [3]. In such contexts, a secure boot process becomes essential for establishing a trusted computing base by ensuring that only authenticated and untampered firmware was executed [4]. This process must verify the digital signature of boot code while consuming minimal power and memory, creating a need for lightweight yet resilient secure boot

mechanisms tailored specifically to embedded systems. The security and reliability of the entire IoT stack hinge on the integrity of this foundational phase [5].

Beyond secure initialization, the management of cryptographic keys across distributed edge devices introduces additional complexity [6]. Traditional models, which depend heavily on centralized certificate authorities or hardware security modules, are increasingly ineffective at scale due to latency, cost, and single points of failure [7]. As edge networks grow denser and more autonomous, the need arises for decentralized key management architectures that support local decision-making and dynamic trust establishment [8]. These architectures must ensure secure key generation, distribution, renewal, and revocation across heterogeneous devices without relying on persistent connectivity or global synchronization [9]. Integrating such systems requires innovative approaches to identity provisioning and trust anchors, particularly in mobile or ad hoc networks where nodes frequently join and leave [10].