RADemics

IoT Security Using Lightweight Cipher Suites in Constrained Application Protocols (CoAP)

Reena Shinde, Bramah Hazela
SINHGAD COLLEGE OF SCIENCE, AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY

IoT Security Using Lightweight Cipher Suites in Constrained Application Protocols (CoAP)

[1]Reena Shinde, Associate Professor, Department of Computer Science, Sinhgad College of Science, Pune, Maharashtra, India. reena.pingale@gmail.com

[2]Bramah Hazela, Assistant Professor, Department of Computer Science and Engineering, Amity School of Engineering and Technology, Lucknow, Amity University Uttar Pradesh. bramahhazela77@gmail.com

Abstract

The rapid expansion of the Internet of Things (IoT) ecosystem has intensified the need for lightweight, yet robust security mechanisms tailored to constrained environments. This book chapter presents a comprehensive investigation into the integration of lightweight cipher suites within the Constrained Application Protocol (CoAP), focusing on cryptographic performance, interoperability, and deployment-specific trade-offs. Emphasizing both symmetric and asymmetric approaches, it explores the selection, benchmarking, and suitability of modern AEAD and lightweight public-key ciphers for microcontroller-based architectures. The chapter examines real-world case studies in industrial automation, healthcare, and smart infrastructure to analyze the practical impact of cipher choices on energy consumption, latency, and security resilience, it delves into challenges such as cipher suite negotiation across heterogeneous CoAP stacks, protocol compatibility, and security versus performance trade-offs. Highlighting the importance of adaptive cryptographic frameworks, the discussion advances the state of secure IoT communications by aligning cryptographic primitives with application and hardware constraints. This work contributes to the evolving discourse on efficient end-to-end protection in resource-constrained networks, paving the way for future scalable and secure IoT systems.

Keywords: CoAP Security, Lightweight Cryptography, AEAD Ciphers, Asymmetric Encryption, IoT Protocols, Resource-Constrained Devices

Introduction

The convergence of the physical and digital worlds through the Internet of Things (IoT) has brought unprecedented connectivity to everyday objects and critical infrastructures [1]. With billions of devices interacting over constrained networks, ensuring secure communication becomes essential. The Constrained Application Protocol (CoAP), standardized by the IETF, provides a lightweight, RESTful communication protocol tailored for constrained environments, supporting low-power operations and small packet sizes over UDP [2]. While CoAP enables scalable and interoperable messaging, it lacks inherent security, making it necessary to integrate external cryptographic mechanisms [3]. Traditional security protocols such as TLS or IPsec, though proven in conventional computing systems, are often too resource-intensive for devices operating with limited CPU power, memory, and battery capacity [4]. As a result, the focus has shifted toward lightweight security frameworks that can effectively protect data integrity, confidentiality, and authenticity without compromising performance [5].

To address this challenge, lightweight cipher suites have been developed and integrated into security protocols optimized for constrained nodes [6]. These include both symmetric key algorithms like AES-CCM and ChaCha20-Poly1305 and asymmetric schemes based on elliptic curve cryptography (ECC), such as Curve25519 [7]. While offering cryptographic strength, these algorithms also meet the efficiency demands of IoT microcontroller platforms [8]. The success of integrating such cipher suites into CoAP-based systems depends on how well they align with the communication protocol's minimalistic design and the device's limited capabilities [9]. Standardized extensions such as OSCORE (Object Security for Constrained RESTful Environments) and EDHOC (Ephemeral Diffie-Hellman Over COSE) further facilitate secure communication using these lightweight ciphers at different layers of the CoAP stack, enabling end-to-end and mutual authentication models [10].