RADemics

Authenticated Encryption Techniques for Secure M2M Communication in IoT

Abdul Razzak Khan Qureshi, Priyanka Jain
MEDICAPS UNIVERSITY

Authenticated Encryption Techniques for Secure M2M Communication in IoT

[1]Abdul Razzak Khan Qureshi, Assistant professor, Department of Computer Science, Medicaps University, Indore, Madhya Pradesh, India. dr.arqureshi786@gmail.com

[2]Priyanka Jain, Assistant Professor, Department of Computer Science, Medicaps University, Indore, Madhya Pradesh, India. priyankajain72222@gmail.com

Abstract

Machine-to-Machine (M2M) communication forms the foundational backbone of the Internet of Things (IoT), enabling autonomous data exchange across diverse devices and platforms. As M2M networks scale rapidly in size and complexity, securing data confidentiality, integrity, and authenticity becomes increasingly critical. Authenticated Encryption with Associated Data (AEAD) offers a robust cryptographic approach to protect both payload and metadata, yet its integration within dynamic, resource-constrained, and high-churn environments introduces substantial challenges. This chapter explores scalable key management strategies and the seamless incorporation of AEAD into secure communication protocols tailored for M2M systems. A comprehensive analysis of key negotiation, lightweight revocation mechanisms, and the applicability of existing standards—such as DTLS, EAP, and IKEv2—is provided. Security risks in hierarchical and mesh-based M2M architectures are examined in detail, emphasizing the need for efficient, adaptive, and lightweight solutions, the chapter presents novel approaches for dynamic key updates and trust-driven revocation protocols that address the limitations of conventional Public Key Infrastructure (PKI) in decentralized IoT contexts. By aligning cryptographic strength with operational scalability, the chapter provides a framework to advance the secure deployment of M2M communication at large scale.

Keywords: Machine-to-Machine (M2M) Communication, Authenticated Encryption (AE), AEAD, Key Management, IoT Security, Lightweight Revocation

Introduction

Machine-to-Machine (M2M) communication has become a cornerstone of modern digital infrastructure, playing a crucial role in enabling devices to interact, exchange data, and respond autonomously without human intervention [1]. It underpins a wide range of applications in sectors such as industrial automation, healthcare, smart cities, transportation, and environmental monitoring. These systems operate across heterogeneous platforms and network conditions, often involving constrained devices with limited computational resources and energy availability [2]. As M2M networks expand and become increasingly decentralized, the attack surface for potential cyber threats also widens [3]. Ensuring end-to-end security in such systems was not merely a functional requirement but a necessity for protecting data integrity, privacy, and system availability [4]. The dynamic and distributed nature of M2M networks necessitates security mechanisms that are not only strong and flexible but also scalable and lightweight, thereby aligning with the operational limitations of typical IoT devices [5].

A key component of secure M2M communication was the deployment of encryption techniques that guarantee confidentiality and authenticity simultaneously [6]. Traditional encryption models often fail to address modern adversarial strategies that exploit metadata exposure or partial message tampering. In this context, Authenticated Encryption with Associated Data (AEAD) offers a compelling solution [7]. AEAD algorithms provide the dual functionality of encryption and message authentication while preserving the verifiability of non-encrypted, associated data such as headers or contextual information [8]. This characteristic was particularly beneficial in M2M scenarios where metadata was necessary for routing or control functions and must remain in plaintext yet verifiably intact [9]. Integrating AEAD within M2M networks was not straightforward due to the unique challenges posed by distributed key management, intermittent connectivity, and real-time communication requirements [10].