RADemics

Lightweight Cryptography and Blockchain Synergies in IoT Trust Management

V. Bhoopathy, Bramah Hazela
SREE RAMA ENGINEERING COLLEGE, AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY

Lightweight Cryptography and Blockchain Synergies in IoT Trust Management

[1]V. Bhoopathy, Professor, Department of Computer Science and Engineering, Sree Rama Engineering College, Tirupathi, India. v.bhoopathy@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 convergence of lightweight cryptography and blockchain technology offers a transformative approach to trust management in the Internet of Things (IoT), particularly within resource-constrained environments. Traditional security models fall short in addressing the dual demands of scalability and efficiency, prompting the need for hybrid frameworks that integrate cryptographic minimalism with decentralized trust mechanisms. This chapter presents a comprehensive design and evaluation of hybrid lightweight blockchain-cryptography frameworks tailored for secure, energy-efficient, and privacy-preserving trust management in distributed IoT networks. It explores system design trade-offs, secure data aggregation techniques, and immutable storage strategies while introducing edge-assisted trust computation to offload intensive operations. Advanced privacy-preserving methods, such as zero-knowledge proofs and differential privacy, are incorporated to mitigate data exposure risks inherent to transparent blockchain infrastructures. The proposed architecture was aligned with practical deployment scenarios and threat models, delivering scalable, low-latency, and tamper-resistant trust infrastructures for heterogeneous IoT ecosystems. The chapter closes by identifying key research gaps and future directions necessary to standardize and optimize such hybrid frameworks across diverse application domains.

Keywords: Lightweight Cryptography, Blockchain, IoT Security, Trust Management, Privacy Preservation, Edge Computing

Introduction

The Internet of Things (IoT) has evolved into a foundational element of modern digital ecosystems, enabling seamless interconnectivity among billions of heterogeneous devices ranging from industrial sensors and medical implants to autonomous vehicles and smart home systems [1]. This proliferation of interconnected devices introduces a wide spectrum of security challenges, including data integrity threats, unauthorized access, and identity spoofing, particularly when traditional security mechanisms are applied [2]. These mechanisms, which often rely on heavyweight cryptographic operations and centralized trust authorities, are not feasible [4]. Resource-constrained environments where power, memory, and computational capabilities are significantly limited [3]. Addressing these issues requires a paradigm shift in trust management, moving towards more adaptive, efficient, and decentralized security models that cater specifically to the unique constraints and requirements of IoT environments [5].

Lightweight cryptography emerges as a viable response to the limitations imposed by low-power and embedded IoT devices [6]. These cryptographic techniques are tailored to provide essential security services—such as confidentiality, authenticity, and integrity—while maintaining a minimal footprint in terms of computation, memory usage, and energy consumption [7]. Unlike traditional encryption methods, lightweight cryptographic primitives are optimized for execution on microcontrollers, field-programmable gate arrays (FPGAs), and other constrained hardware platforms [8]. Their advantages, these techniques alone are insufficient to ensure trust across large-scale, dynamic IoT networks due to their limited capacity to support auditability, tamper resistance, and global consensus [9]. Consequently, integrating these mechanisms with decentralized trust infrastructures becomes necessary to enhance transparency, traceability, and system-wide security guarantees [10].