Study on the Enhancement of Scalability, Security, and Privacy in IoT Systems with Practical Blockchain-Based Access Control

Name : Christopher Wiraatmaja

Laboratory's name : Large-Scale Systems Management

Supervisor's name : Prof. Shoji Kasahara

Abstract

In this dissertation, we investigate multiple approaches to enhancing the scalability, security, and privacy of blockchain-based access control systems for the Internet of Things (IoT). First, we improve the cost-efficiency of Blockchain-Based Attribute-Based Access Control (ABAC) by integrating blockchain oracles and decentralized storage, reducing operational costs while maintaining robustness. Subsequently, we introduce zero-knowledge set-membership proofs into blockchain-based authentication, enabling anonymous authentication requests with strong privacy guarantees, superior cost-efficiency, and competitive latency compared to existing schemes. Finally, we leverage the Lookup Argument, a recent advancement in zero-knowledge proofs, to significantly enhance the efficiency of Blockchain-Based ABAC. This allows us to design a scalable yet anonymous ABAC system optimized for complex IoT ecosystems. Our results demonstrate orders-of-magnitude improvements in proving time, exceeding 1000x in more complex policies, making the proposed scheme particularly suitable for resource-constrained IoT devices.