Journal Name: Journal of Industrial Information Integration **IF: 10.4**

Title: A Blockchain assisted fog computing for secure distributed storage system for IoT Applications

Author: Apat H.K.; Sahoo B.

Details: Volume 42, November 2024, Article number 100739

Abstract: With the rapid development of Internet of Things (IoT) devices, the volume of data generate across various fields, such as smart healthcare, smart home, smart transportation has significantly increased. This surge raises serious concerns about the secure storage of sensitive data for e.g., biometric information (e.g., fingerprints and facial recognition) and medical records etc. The centralized cloud computing paradigm provides various cost-effective services to IoT applications users. Despite of various benefits of centralized cloud, it fails to adequately meet the strict latency and security requirement of various IoT applications. Fog computing is proposed to enhance the real-time data processing for various latency sensitive IoT applications by extending the cloud computing services closer to the data sources. In this paper we proposed a novel blockchain based distributed fog computing model that ensures secure distributed storage for various IoT data. The blockchain network acts a trusted third party aimed at establishing secure communication among IoT devices and fog node within the fog layer. It details a distinctive Elliptic Curve Diffie–Hellman (ECDH) protocol for reliable and secure data storage and retrieval based on requests and responses from heterogeneous IoT devices. Additionally, a Merkle tree-based data structure is used to verify data integrity, ensuring secure and tamper-proof data management within the blockchain-enabled fog computing framework. It provides a formal security proof using AVISPA tools for the proposed scheme, ensuring that it meets the necessary security standards and can be trusted for protecting sensitive IoT data. Finally, the proposed scheme is compared with existing security schemes, such as AES, ABE, RSA, and Hybrid RSA in terms of resource utilization, computational cost, communication cost and execution cost. The experimental results exemplify that the proposed scheme outperform other state of the art schemes.

URL: https://www.sciencedirect.com/science/article/pii/S2452414X24001821?via%3Dihub