Peer-to-Peer Networking and Applications (2024) 17:3905–3933
https://doi.org/10.1007/s12083-024-01801-z

Securing IoT data: Fog computing, blockchain, and tailored privacy-enhancing technologies in action

Iraq Ahmad Reshi[1] · **Sahil Sholla**[1]

Received: 6 March 2024 / Accepted: 27 August 2024 / Published online: 7 September 2024

Abstract

The inherent challenges associated with the Internet of Things (IoT), such as vulnerability to cyber threats and privacy issues, need the development of novel solutions to ensure secure and efficient handling of data. Fog computing resolves these concerns by facilitating data processing in proximity to edge devices, minimising latency, and improving real-time decision-making. Blockchain boosts security in fog-based systems by providing a tamper-proof and transparent ledger. However, exclusively prioritising privacy in fog-based blockchains may impede the practical execution. This article presents the FogBlock Connect paradigm, which combines Fog computing and Blockchain through the implementation of a tailored Proxy Re-encryption (PRE) algorithm inspired by BBS98. This strategy guarantees enhanced data confidentiality while simultaneously upholding operational effectiveness in fog-based blockchains for Internet of Things applications. The efficiency and effectiveness of the suggested PRE algorithm over typical encryption methods are confirmed by comprehensive simulations utilising the Fobsim simulator. The FogBlock Connect paradigm entails the transmission of updates from nearby IoT devices to Fog servers for the purpose of creating and securely storing global updates, hence improving efficiency and performance. The paradigm ensures robust privacy measures, mitigates risks of single-point failures, and facilitates precise access control, establishing a basis for secure and resilient IoT applications. The CCA resistant formal security proof provides further validation for the strength and effectiveness of the suggested approach.

Keywords Proxy re-encryption · Fog computing · Blockchain · Edge-IoT · Smart contracts

1 Introduction

The Internet of Things (IoT) emerged from the interconnection of physical items , leading to swift progress in communication, data processing, and technological breakthroughs[1]. Its applications embrace diverse disciplines, including healthcare, agriculture, transportation, and smart home technology, to improve human existence [2]. The rise in utilisation of IoT devices may primarily be due to two crucial factors: the declining prices of processing and the broad availability of wireless connectivity [3]. Various industries, are progressively utilising the IoT and cloud computing services to monitor critical applications such as industrial control systems and smart grids. The main objective is to enhance efficiency and reduce operational costs [1, 2, 4].The essential data of the IoT is stored within a third-party cloud service provider as part of the conventional architecture for IoT-cloud integration [3].Nevertheless, integrating these devices present challenges, particularly in managing the limited resources available for interconnected devices and addressing concerns regarding the possible vulnerability of sensitive IoT data [4]. It is important to recognise that cloud servers, essential to the traditional IoT-cloud structure, possess extensive knowledge of the data they store, which leads to privacy concerns. Researchers are currently working on methods to tackle these problems and enhance system performance in terms of stability, adaptability, fault tolerance, and cost-effectiveness [3].

Nevertheless, the conventional cloud-based architecture for IoT encounters substantial challenges, notably as a result of vulnerabilities in smart devices. The vulnerabilities mostly arise from the small storage capacities and computing power of these devices, rendering current secure communication

This article is part of the Topical Collection: *4 - Track on IoT*
Guest Editor: Peter Langendoerfer

✉ Iraq Ahmad Reshi
rshiraq333@gmail.com

[1] Department of CSE, Islamic University of Science and Technology, Awantipora, Kashmir, J&K, India