A Comprehensive Review of Proxy Encryption Concept and Implementation for Safe Blockchain-based IoT Data Sharing

Miss. Sudhatai Vitthal Harale[1] and Prof. Shubhangi S. Mandwale[2]

Department of Artificial Intelligence and Machine Learning[1,2]

Shreeyash College of Engineering & Technology, Chh. Sambhajinagar

Abstract: *The rapid growth that comprise the Internet of Things (IoT) has made data sharing is among cloud computing's most useful uses. However, despite its potential, data security remains a significant challenge, as unauthorized access can result in severe consequences. This work introduces solution that allows for safe data sharing in cloud environments through proxy re-encryption. Before transferring data to the cloud, owners encrypt it using identity-based encryption. To restrict access to authorised users exclusively, a proxy re-encryption technique is used. Considering the resource limitations of IoT devices, computationally demanding operations are offloaded to an edge device functioning as a proxy server. Additionally, by leveraging information-centric networking, cached content can be efficiently delivered through the proxy, enhancing network bandwidth utilization and improving service quality. The proposed system integrates blockchain technology to provide decentralized data sharing and fine-grained access control, overcoming the drawbacks of traditional centralized approaches. Security examinations and assessments of performance show that the plan effectively preserves data confidentiality, integrity, and overall security.*

Keywords: Internet of Things, Cloud Computing, Data Security, Proxy Re-Encryption, Identity-Based Encryption, Edge Computing