A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain

ABSTRACT

The evolution of the Internet of Things has seen data sharing as one of its most useful applications in cloud computing. As eye-catching as this technology has been, data security remains one of the obstacles it faces since the wrongful use of data leads to several damages. In this article, we propose a proxy re-encryption approach to secure data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while proxy re-encryption construction will grant legitimate users access to the data. With the Internet of Things devices being resource-constrained, an edge device acts as a proxy server to handle intensive computations. Also, we make use of the features of information-centric networking to deliver cached content in the proxy effectively, thus improving the quality of service and making good use of the network bandwidth. Further, our system model is based on blockchain, a disruptive technology that enables decentralization in data sharing. It mitigates the bottlenecks in centralized systems and achieves fine-grained access control to data. The security analysis and evaluation of our scheme show the promise of our approach in ensuring data confidentiality, integrity, and security.

**EXISTING SYSTEM**

Park [16] provided a modification to the scheme in [15], where collusion between the service provider and revoked users is avoided. Their scheme was to basically replace the service provider with a trusted third party, which implies that there should be reliance on stronger trust assumption. Other schemes [17]–[19] have made similar approaches but utilized ciphertext-policy ABE (CP-ABE) rather, in which the access policy is associated with the ciphertext instead of the secret keys. Liu *et al.* [20] also proposed a time-constrained access control scheme based on PRE and ABE. ABE was used to design time-based access control policies while PREwas used to update the time attributes. Although these schemes have their advantages, they are not suitable in the context of IoT due to the heavy computations on encryption and decryption.

An IBE PRE scheme suitable for data sharing was presented by Han *et al.* in [21]. The re-encryption keys were not only bound to the users’ identities but also to a specific ciphertext. This implied that the data owner had to create a different reencryption key for each pair of data user and shared file. A similar idea was proposed by Lin *et al.* [22] where they used a hierarchical PRE instead of an identity-based PRE. These two schemes tend to be inefficient when multiple and complex data pieces are considered. An identity-based broadcast encryption (IBBE) combined with PRE was proposed by Zhou *et al.* in [23] for data sharing. Their scheme was a hybrid one that allowed the conversion to be done between the two protocols without

leaking any sensitive information.Wang *et al.* [24] also designed an identity-based PRE (IBPRE) scheme for accessing health records. The scheme achieved coarse-grained access control.

If a proxy receives the re-encryption key from the data owner, either all the ciphertexts can be re-encrypted and accessible to the intended users or none at all. On that note, Shao *et al.* [25] proposed an IBEPREscheme that is based on conditions. In their proposal, the proxy could transform a subset of ciphertexts under an identity to other ciphertexts under another identity. However, decryption rights to a group of users could not be authorized. In addition to the above, PRE has been used to mitigate security problems in IoT [26].

Zyskind *et al.* [27] used blockchain to provide distributed personal data management and ensure privacy as well. The blockchain was utilized as an automatic access control manager, and, hence, no third party was required. Only the data address was stored on the blockchain and a distributed hash table was used as the implementation of the data storage. This reduced the risk of data leakage.

Fan *et al.* [29] designed a similar model to [28] where the encrypted data is uploaded to the cloud and access policies on the data are stored on the blockchain as transactions. Although these two schemes achieve tamper-proof systems and easy auditing, there is a leakage of access policies since the blockchains used are public ones and are thus visible to everyone. Singh and Kim [30] presented a blockchain-based model for sharing data in vehicular networks and also enable secure communication among vehicles. However, the use of a public blockchain does not work well in peer-to-peer (P2P) data sharing among vehicles due to the high cost involved in establishing a public blockchain in resource-constrained vehicles.

Disadvantages

1) The system was not implemented Attribute Based Encryption Mentod which leads less security on outsourced data.

2) The system is less security due to lack of Identity-Based Encryption.

**PROPOSED SYSTEM**

* The system proposes a secure access control framework to realize data confidentiality, and fine-grained access to data are achieved. This will also guarantee data owners’ complete control over their data.
* The system gives a detailed description of our PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.
* To improve data delivery and effectively utilize the network bandwidth, edge devices serve as proxy nodes and perform re-encryption on the cached data. The edge devices are assumed to have enough computation capabilities than the IoT devices and as such provide high performance networking.
* The security analysis of our scheme is presented, and we also test and compare its performance with existing schemes.

**Advantages**

1) The proposed system is secure against man-in-the-middle (MITM) attacks. MITM attacks get to the certificate authority (CA) to provide the user with forged public keys.

2) The proposed system finds Data Tampering and blocks when hackers compromise a system, they inject their own versions of the data into the system.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL