A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era

Aftab Ansari
Student
Oriental University

ABSTRACT

A cloud-based big data sharing system utilizes a storage facility from a cloud service provider to share data with legitimate users. In contrast to traditional solutions, cloud provider stores the shared data in the large data centers outside the trust domain of the data owner, which may trigger the problem of data condentiality. This paper proposes a secret sharing group key management protocol (SSGK) to protect the communication process and shared data from unauthorized access. Different from the prior works, a group key is used to encrypt the shared data and a secret sharing scheme is used to distribute the group key in SSGK. The extensive security and performance analyses indicate that our protocol highly minimizes the security and privacy risks of sharing data in cloud storage and saves about 12% of storage space.

EXISTING SYSTEM

❖ Rao [19] proposed a secure sharing schemes of personal health records in cloud computing based on ciphertextpolicy attributed-based(CP-ABE) signcryption [20]. It focus on restricting unauthorized users on access to the confidential data. Liu *et al.* [21] proposed an access control policy based on CP-ABE for personal records in cloud computing as well. In [19] and [21],only one fully trusted central authority in the system is responsible for key management and key generation.

❖ Huang *et al.* [22] introduced a novel public key encryption with authorized equality warrants on all of its ciphertext or a specified ciphertext. To strengthen the securing requirement, Wu *et al.* [23] proposed an efficient and secure identity-based encryption scheme with equality test in cloud computing. Xu *et al.* [24] proposed a CP-ABE using bilinear pairing to provide users with searching capability on ciphertext and fine-grained access control. He *et*

al. [25] proposed a scheme named ACPC aimed at providing secure, efficient and fine grained data access control in P2P storage cloud.

❖ Recently, Xue *et al.* [26] proposed a new framework, named RAAC, to eliminate the single-point performance bottleneck of the exiting CP-ABE based access control schemes for public cloud storage. While these schemes use identity privacy by using attribute-based techniques which fail to protect user attribute privacy.

❖ The most recent work addressing the privacy issues in a cloud-based storage is carried out by Pervez *et al.* [27], who proposed a privacy aware data sharing scheme SAPDS. It combines the attribute based encryption along with proxy re-encryption and secret key updating capability without relying on any trusted third party. But the storage and communication overhead of SAPDS is decided by attribute encryption scheme.

Disadvantages

- In the existing work, there is no group based access control system.
- The system's security is very less due to lack of strong cryptography techniques.

PROPOSED SYSTEM

In SSGK, an efcient solution is proposed to solve the secure problems of data sharing on the cloud storage without relying on any trust third party. Beyond using symmetric encryption algorithm [11] to encrypt the shared data, asymmetric algorithm [12] and secret sharing scheme [28], [29] is used to prevent the key used to decrypt the shared data from getting by unauthorized users. Secret sharing schemes were introduced by both Blakley [30] and Shamir [31] independently in 1979 as solution for safe guarding cryptography
keys. In a secret sharing scheme, a secret is divided into n shares by a dealer and shared among n shareholders. Any t shares can reconstruct this secret. Chor et al. [32] extended the notion of the original secret sharing and presented a notion of verifiable secret sharing (VSS). The property of verifiability means that shareholders are able to verify whether their shares are consistent.

Advantages

➢ The data owner is totally trusted and will never be corrupted by any adversaries.

➢ The system is more secured due to the group key is distributed by running the secret sharing scheme. Parts of the group members can gather their sub secret shares to reconstruct the group key.