A SECURE AND VERIFIABLE ACCESS CONTROL SCHEME FOR BIG DATA STORAGE IN CLOUDS

ABSTRACT

- Due to the complexity and volume, outsourcing ciphertexts to a cloud is deemed to be one of the most effective approaches for big data storage and access.
- Nevertheless, verifying the access legitimacy of a user and securely updating a ciphertext in the cloud based on a new access policy designated by the data owner are two critical challenges to make cloud-based big data storage practical and effective.
- Traditional approaches either completely ignore the issue of access policy update or delegate the update to a third party authority.

- In this paper, we propose a secure and verifiable access control scheme based on the NTRU cryptosystem for big data storage in clouds. We first propose a new NTRU decryption algorithm to overcome the decryption failures of the original NTRU,and then detail our scheme and analyze its correctness, security strengths, and computational efficiency.
- Our scheme allows the cloud server to efficiently update the ciphertext when a new access policy is specified by the data owner, who is also able to validate the update to counter against cheating behaviors of the cloud.

EXISTING SYSTEM

- Most existing approaches for securing the outsourced big data in clouds are based on either attributed-based encryption or secret sharing. ABE based approaches provide the flexibility for a data owner to predefine the set of users who are eligible for accessing the data but they suffer from the high complexity of efficiently updating the access policy and ciphertext.
- Secret sharing mechanisms allow a secret to be shared and reconstructed by certain number of cooperative users but they typically employ asymmetric public key cryptograph such as RSA for users' legitimacy verification, which incur high computational overhead.

Disadvantages

- Its complexity and large volume, managing big data using on hand database management tools is difficult.
- It is also a challenging issue to dynamically and efficiently update the access policies according to the new requirements of the data owners in secret sharing approaches

PROPOSED SYSTEM

- We propose a new NTRU decryption procedure to over-come the decryption failures of the original NTRU without reducing the security strength of NTRU.
- We propose a secure and verifiable access control scheme to protect the big data stored in a cloud. The scheme can verify a user's access legitimacy and validate the information provided by other users for correct plaintext recovery.
- We devise an efficient and verifiable method to update the ciphertext stored in clouds without increasing any risk when the access policy is dynamically changed by the data owner for various reasons.

Advantages

- The proposed scheme should be able to defend against various attacks such as the collusion attack
- To reduce the risk of information leakage.

Conclusion

- In this paper, we first propose an improved NTRU cryptosystem to overcome the decryption failures of the original NTRU and then present a secure and verifiable access control scheme based on the improved NTRU to protect the outsourced big data stored in a cloud. Our scheme allows the data owner to dynamically update the data access policy and the cloud server to successfully update the corresponding outsourced ciphertext to enable efficient access control over the big data in the cloud.