A NOVEL EFFICIENT REMOTE DATA POSSESSION CHECKING PROTOCOL IN CLOUD STORAGE

ABSTRACT

- As an important application in cloud computing, cloud storage offers user scalable, flexible and high quality data storage and computation services.
- A growing number of data owners choose to outsource data files to the cloud.
- Because cloud storage servers are not fully trustworthy, data owners need dependable means to check the possession for their files outsourced to remote cloud servers.
- To address this crucial problem, some remote data possession checking (RDPC) protocols have been presented.
- But many existing schemes have vulnerabilities in efficiency or data dynamics.

CONTD…

- In this paper, we provide a new efficient RDPC protocol based on homomorphic hash function.
- The new scheme is provably secure against forgery attack, replace attack and replay attack based on a typical security model.
- To support data dynamics, an operation record table (ORT) is introduced to track operations on file blocks.
- We further give a new optimized implementation for the ORT which makes the cost of accessing ORT nearly constant.
- Moreover, we make the comprehensive performance analysis which shows that our scheme has advantages in computation and communication costs.

DOMAIN

- **Information security**, sometimes shortened to **InfoSec**, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).
- **Network security** consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

Cont…

- Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals.
- Networks can be private, such as within a company, and others which might be open to public access.
- Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains:
- It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Existing System

- Cloud service provider tries to provide a promising service for data storage, which saves the users costs of investment and resource. Nonetheless, cloud storage also brings various security issues for the outsourced data.
- Although some security problems have been solved the important challenges of data tampering and data lost are still existing in cloud storage.
- On the one hand, the accident disk error or hardware failure of the cloud storage server (CSS) may cause the unexpected corruption of outsourced files.
- On the other hand, the CSS is not fully trustworthy from the perspective of the data owner, it may actively delete or modify files for tremendous economic benefits.
- At the same time, CSS may hide the misbehaviors and data loss accidents from data owner to maintain a good reputation.

DISADVANTAGES

- It is crucial for the data owner to utilize an efficient way to check the integrity for outsourced data.
- In addition, they supplied two concrete schemes (S-PDP, E-PDP) based on RSA. Although these two protocols had good performance, it's a pity they didn't support dynamic operations.
- Does not provide efficiency in remote data integrity checking.
- More expensive.
- The existing system provides less flexibility.

PROPOSED SYSTEM

- To find the location of each data Merkle Hash Tree is used. A third party auditor can also be called as trusted party auditor checks the user's data stored in cloud storage for its correctness and accuracy.
- A third party ensures correctness of user's data. Many times verification is allowed without the requiring the verifier to compare against the original data.
- They incur less computation and communication cost. Enhanced security and performance analysis shows that the proposed scheme is more efficient and strong against replace attack launched by malicious server.

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Gener. Comp. Sy., vol. 25, no. 6, pp. 599 – 616, 2009.

[2] H. Qian, J. Li, Y. Zhang and J. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," Int. J. Inf. Secur., vol. 14, no. 6, pp. 487-497, 2015.

[3] J. Li, W. Yao, Y. Zhang, H. Qian and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016.2520932.

[4] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage," IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016. 2542813.

[5] J. Li, Y. Shi and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," Int. J. Commun. Syst., DOI: 10.1002/dac.2942.

[6] J.G. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no.11, pp. 2150-2162, 2012.