Component-Based Framework For Exchanging Information In Blockchain Using Sepse

R.Manivannan[1], K. Balasubramanian[2], M. Markco[3], A.Udhaya Veena[4]

Associate Professor[1,2], Assistant Professor[3], PG Scholar[4]

Department of Computer Science and Engineering, E. G. S. Pillay Engineering College, Nagapattinam

Abstract

This project to propose a dynamic audit service for authenticating the integrity of un-trusted and outsourced storage. This verifies service is created based on the procedures like portion structure, arbitrary sampling, and hash, supporting provable updates to outsourced data and timely anomaly detection. In addition, to propose a method based on the probabilistic query and periodic verification for improving the performance of audit services. These experimental results not only validate the effectiveness of these approaches but also show our audit system which verifies the integrity with lower computation overhead and requiring less storage for audit metadata. Another main concern is the safety issue of dynamic data processes for public audit services, so we present a secure and efficient PEKS scheme called SEPSE against KGA, where users encrypt keywords with the aid of dedicated key servers via a threshold and oblivious way. SEPSE supports key renewal to periodically replace an existing key with a new one on each key server to thwart the key compromise. The blockchain is a new technology for data sharing between un-trusted peers Blockchain has solved the problem of changing the original low-trust centralized ledger held by a single third-party, to a high-trust decentralized form held by different objects, or in other words, verifying nodes.

Keywords: Dynamic audit, Arbitrary sampling, Hash function, KGA, PEKS, SEPSE.

1. INTRODUCTION

With cloud storage services, users can outsource their data to the remote storage server and flexibly access them via the Internet. Such services also provide users an efficient way to send their data to others. Typical applications include store-and-forward systems, such as cloud-based email systems, where multiple users (called senders) are willing to send data containing a small number of keywords to one user (called receiver). Senders are able to outsource the data as well as keywords to the storage server, and the receiver can retrieve target data from the storage server through searching by keywords. Furthermore, we propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. A proof-of-concept prototype is also implemented to evaluate the feasibility and viability of our proposed approaches. After verifying the trust parameters of the outsource data, the kind of blockchain concept was introduce. In the past, blockchain were commonly associated with digital currencies such as Bitcoin, or alternate versions of Bitcoin like Bitcoin Cash. Today, blockchain applications are being explored in many industries as a secure and cost-effective way to create and manage a distributed database and maintain records for digital transactions of all types. Along with blockchain secure and efficient searchable public key encryption scheme was used. Because of the key guessing attacks(KGA) SEPSE scheme was used

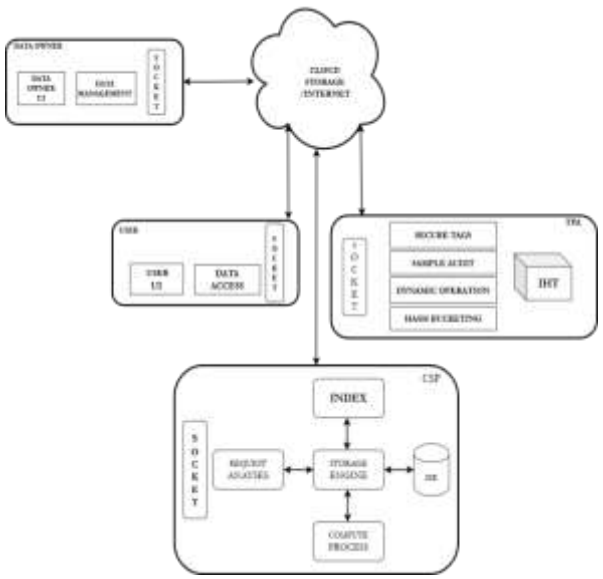
2. METHODS AND PROCESS

To finding the problem in cloud infrastructure to retrieve and uploading data are more powerful and reliable than personal computing devices, but they are still susceptible to

internal threats. Occasionally affected from the lack of trust on CSP because the data change. so the security audit is an important solutions enabling trace back and analysis of any activities including data access, security breaches and application activities. Also suffer from keyword guessing attack wherein attacker first generates encrypted tags corresponding to all possible keywords.However the accuracy of the data to fight against over KGA attack and data security tracking A Bucketing hashing-based technique, called flexible Bucketing-based hashing, for processing the NN query. The main advantage of this technique is that the server always returns an exact binary candidate set for the key. The client then refines the candidate set to obtain the final result.so we also find the result as well from the key attack.

3. SYSTEM OVERVIEW

In this work the existing algorithm has been modified and introduces hands on technique dynamic audit service for integrity verification of un-trusted and outsourced storages. These audit service can provide public audit ability without downloading raw data and protect privacy of the data.Also, this audit system can support dynamic data operations and timely anomaly detection with the help of several effective techniques, such as fragment structure, random sampling, and Index-Hash Table (IHT), also propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. the generation of server-derived keyword can be distributed over multiple key servers via a threshold secret sharing protocol,the blockchain along with dynamic audit service. we propose the SEPSE,Secure and Efficient Searchable Public Key Encryption. scheme is a key technique for protecting data confidentiality.This SEPSE scheme proven under the rigorous security definition.



Our main contributions of this paper are:

(i)Fragment Structure And Secure Tags Creation Module To maximize the storage efficiency and audit performance, our audit system introduces a general fragment structure for outsourced storages. An outsourced file F is split into n blocks $\{M_1, M_2, \ldots . M_n\}$, and each block mi is split into s sectors $\{M_1, M_2, \ldots . M_{i,s}\}$.The fragment framework consists of n block-tag pair (M_i, σ_i), where σ_i is a signature tag of a block mi generated by some secrets $\tau = (\tau_1, \tau_2, \ldots . \tau_s)$. Use such tags and corresponding data to construct a response in terms of the TPA's challenges in the verification protocol, such that this response can be verified without raw data. If a tag is un-forgeable by anyone except the original signer, we call it a secure tag.

(ii)Periodic Sampling Audit Module In this module with "whole" checking, random "sampling" checking greatly reduces the workload of audit services, while still achieves an effective detection of misbehaviors. Thus, a probabilistic audit on sampling checking is preferable to realize the anomaly detection in a timely manner.

(iii)**Index-Hash Table creation Module** To support dynamic data operations, we introduce a simple IHT to record the changes of file blocks, as well as generate the hash value of each block in the verification process. The structure of our IHT is similar to that of file block allocation table in file systems. Generally, the IHT consists of serial number, block number, version number, and random integer.

(iv)**Dynamic Data Operations Module** Dynamic data operations are available only to DOs or AAs, who hold the secret key sk. Here, all operations are based on data blocks. Moreover, to implement audit services, applications need to update the IHTs. It is necessary for TPA and CSP to check the validity of updated data.

(v) **Hash Bucketing Based Knowledge module(SEPSE process)** A Bucketing hashing-based technique, called flexible Bucketing-based hashing, for processing the NN query. The main advantage of this technique is that the server always returns a exact binary candidate set for the key . The client then refines the candidate set to obtain the final result.so we also find the result as well from the key attack.

4.EXPERIMENTAL EVALUATION

The project implementation using dynamic audit and blockchain concept to finding the data security issues and fighting over with KGA attack. The secure public key encryption Secure and Efficient Searchable Public Key Encryption scheme is a key technique for protecting data confidentiality. This SEPSE scheme proven to be secure under a rigorous security definition.

First the process of evaluation is to login and for that login purpose to create a account after that we generate a tag for file block conversion with public key and private key to encrypted the data from the data owner side. To finishing the process we verifying the trustworthy of the data that we upload.

5.CONCLUSION

A construction of dynamic audit services for un-trusted and outsourced storages along with SEPSE . We also presented an efficient method for periodic sampling audit to enhance the performance of TPAs and storage service providers. This project developed in Windows Azure Cloud, mainly this cloud improves the security and performance. Secure and Efficient Searchable Public Key Encryption scheme is a key technique for protecting data confidentiality.This SEPSE scheme proven to be secure under a rigorous security definition.

6. REFERENCES

[1] H. Yang, X. Wang, C. Yang, X. Cong, and Y. Zhang, “Securingcontent-centric networks with content-based encryption,” Journalof Network and Computer Applications, vol. 128, pp. 21–32, 2019.

[2] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, “Enabling efficient andgeometric range query with access control over encrypted spatialdata,” IEEE Trans. Information Forensics and Security, vol. 14, no. 4,pp. 870–885, 2019.

[3] Y. Zhang, C. Xu, X. Lin, and X. Shen, “Blockchain-based publicintegrity verification for cloud storage against procrastinatingauditors,” IEEE Transactions on Cloud Computing, accepted 2019,to appear, doi: 10.1109/TCC.2019.2908400

[4] X. Liu, R. Deng, K. R. Choo, and Y. Yang, “Privacy-preservingoutsourced support vector machine design for secure drug discovery,”IEEE Trans. Cloud Computing, accepted 2018, to appear,doi10.1109/TCC.2018.2799219

[5] A. Yang, J. Xu, J. Weng, J. Zhou, and D. S. Wong, “Lightweightand privacy-preserving delegatable proofs of storage with datadynamics in cloud storage,” IEEE Trans. Cloud Computing, accepted2018, to appear, doi: 10.1109/TCC.2018.2851256.

[6] Y. Zhang, X. Lin, and C. Xu, “Blockchain-based secure data provenance for cloud storage,” in Proc. ICICS, 2018, pp. 3–19

[7] Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo, “Efficienttraceable authorization search system for secure cloud storage,”IEEE Trans. Cloud Computing, accepted 2018, to appear, doi.10.1109/TCC.2018.2820714.

[8] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, “Querying in internetof things with privacy preserving: Challenges, solutions andopportunities,” IEEE Network, vol. 32, no. 6, pp. 144–151, 2018

[9] C. B¨osch, P. Hartel, W. Jonker, and A. Peter, “A survey of provablysecure searchable encryption,” ACM Computing Surveys, vol. 47,no. 2, pp. 1–51, 2014, article. 18.