International Journal of Scientific Research and Engineering Development-– Volume3 Issue 1, Jan-Feb 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Security In Infra Cloud Storage with Sensitive Information Hiding

Asha Elsa George[1], Vineeth M V[2], Smita C Thomas

[1]P. G Scholar, Dept of CSE, Mount Zion College of Engineering, Kadammanitta, Kerala, India

[2]Assistant Professor, Dept of CSE, Mount Zion College of Engineering, Kadammanitta, Kerala, India

3Research Scholar, Vels University, India

----------**********----------

Abstract:

With cloud storage services, users can remotely store their data to the cloud and realize the info sharing with others. Remote data integrity auditing is proposed to guarantee the integrity of the data stored within the cloud. In some cloud storage systems, the cloud file might contain some sensitive information. It makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing remains ready to be efficiently executed. This scheme is based on identity based cryptography, which simplifies the complications. WA-RRNS is used to unravel the matter of security issues, which mixes weighted access scheme and threshold secret sharing redundant residue number system with multiple failure detection or recovery mechanisms.

Keywords **— Cloud storage securities, Data integrity auditing, Data sharing, Sensitive information hiding, Reliability.**

----------**********----------

I. INTRODUCTION

With the explosive growth of data, it is a heavy burden for users to store the sheer amount of data locally. Therefore, more and more organizations and individuals would like to store their data in the cloud. However, the data stored in the cloud might be corrupted or lost due to the inevitable software bugs, hardware faults and human errors in the cloud. In order to verify whether the data is stored correctly in the cloud, many remote data integrity auditing schemes have been proposed. In remote data integrity auditing schemes, the data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures are used to prove the cloud truly possesses these data blocks in the phase of integrity auditing. And then the data owner uploads these data blocks along with their corresponding signatures to the cloud. The data stored in the cloud is often shared across multiple users in many cloud storage applications, such as Google Drive, Dropbox and iCloud. Data sharing as one of the most common features in cloud storage, allows a number of users to share their data with others. However, these shared data stored in the cloud might contain some sensitive information.

To improve the reliability of data storage, propose to use the threshold secret sharing scheme based on redundant residue number system (RRNS), where each cloud has several short shares. This approach allows us to distribute data among clouds, based on their probability of denying data access and failures. The advantage of using RRNS is that it has properties of error correction codes at To improve the security and reliability of storage systems, AR- RRNS, DepSky, and RACS use distributed storage mechanisms based on secret sharing schemes and error correction codes, which spread data over multiple cloud storage provider (CSP). Data chunks allocated to CSPs have

approximately the same size. These schemes reduce the load of the transmission network compared to the classical replication mechanism. However, they do not take into account the probability of failure of each cloud.

Despite extensive research and industry attention in the field of security and reliability of data storage, the probability of data loss is still unacceptable. Cloud providers offer services with varying degrees of reliability. Additional costs may be associated with the required levels of reliability. Therefore, the amount of data stored in each cloud provider is advisable to be proportional to cloud reliability.

To improve the reliability of data storage, propose to use the threshold secret sharing scheme based on redundant residue number system (RRNS), where each cloud has several short shares. This approach allows us to distribute data among clouds, based on their probability of denying data access and failures. The advantage of using RRNS is that it has properties of error correction codes, homomorphic ciphers, and secret sharing schemes at the same time. The multi-cloud distributed storage systems help to minimize the risks of a complete data loss.

The probability of a complete data loss depends directly on the quality of hard disks. Reliability can be increased, when the distributed storage scheme based on threshold secret sharing of RRNS is used. The methods of probability theory, mathematical statistics, stochastic and fuzzy methods are used to solve issues associated with uncertainties. Other approaches use information about previously completed tasks with Machine Learning (ML) methods such as regression, decision trees, etc.. The major issues related to data security include data integrity, data availability, data confidentiality, privacy, transparency of data and control over data where data resides. There are various aspects for providing data security like by providing access controls and encryption methods.

II. LITERATURE SURVEY

The personal sensitive information should not be exposed to remote data integrity auditing still able to be effectively performed. During the process of sanitization, the sanitizer does not need to interact with data's in bulk, and uploads these sanitized data's to the cloud at a fixed time. Firstly, after the data blocks corresponding to the patient's sensitive information are the sensitive information contains two parts. One is the personal sensitive information; other is the organization's sensitive information. Sensitive information should be replaced with wildcards when the datas are uploaded to can be ensured corresponding to the sensitive information such as name by using wildcards, which protects the datas sanitizer. And all the sensitive information should not be exposed to the cloud and the shared users. needs to generate and send the informations of user to the sanitizer for storing them in the information system. However, these Secondly, the sanitizer can facilitate the information management. It can sanitize the the sanitized. It makes the Finally, the sanitizer uploads these sanitized and their corresponding signatures to the cloud.

In this way, the EHRs can be shared and used by researchers, while the sensitive information of EHRs can be hidden. Meanwhile, the integrity of these data stored in the cloud privacy blinded, the contents of these data blocks might become messy code. The sanitizer can unify the format by using wildcards to replace the contents of these data blocks. In addition, the sanitizer also can sanitize the data blocks the sanitizer is necessary because of the Thirdly, when the medical doctor needs the data, the sanitizer as the administrator sensitive information. Generally, these data blocks are replaced with wildcards. Furthermore, the sanitizer can transform these data blocks signatures into valid ones for the sensitive information. The multi-cloud distributed storage systems help to minimize the risks of a complete data loss. The probability of a complete data loss depends directly on the quality of hard disks. The distributed storage scheme based on threshold secret sharing of RRNS is used. datas usually contain the sensitive information. To preserve the privacy of patient from the sanitizer, it blinds the sensitive information of each data before sending this to the sanitizer. Then the server generates signatures for this blinded data and sends them to the sanitizer. The sanitizer stores these

messages into information system. When the user needs the data, he sends a request to the sanitizer. And then the sanitizer downloads the blinded data from the information system and sends it to the medical doctor. Finally, the data recovers the original data from this blinded data. When this data needs to be uploaded and shared in the cloud for research purpose, in order to unify the format, the sanitizer needs to sanitize the data blocks corresponding to the information cloud for research purpose. The sanitizer can be viewed as the administrator of the information system. In addition, to protect the privacy of hospital, the sanitizer needs to sanitize the data blocks corresponding to the administrator sensitive information. Generally, these data blocks are replaced with wildcards. Furthermore, the sanitizer can transform these data blocks' signatures into valid ones for the sensitive information hiding.

III. PROPOSED SYSTEM

To reduce the damage of users key exposure, proposed key-exposure resilient remote data integrity auditing schemes based on key update technique. It is constructed a remote data integrity auditing scheme with perfect data preserving in identity based cryptosystems. It is proposed an identity based satisfying unconditional anonymity and incentive. This paper propose an identity based remote data integrity auditing scheme for shared data supporting cloud, multi cloud informations such as users name or email address to replace the public key. It is designed a remote data integrity auditing schemes that realizes data sharing with sensitive information hiding. The proposed scheme uses identity based remote data integrity real user revocation. This scheme used the users identity. Encrypting the whole shared file can realize the user firstly blinds the data and generates signatures. To solve the security issues, WARRNS method is used to combine weighted access scheme and threshold secret sharing redundant residue number system with multiple failure detection or recovery mechanism and homomorphic ciphers. For better tradeoffs between the security and performance, WARRNS uses parameters to adjust redundancy, encryption decryption speed, data loss probability.
The idea is to split a master secret among some members by providing each member with a share of the secret system, the coalition with a number of shares that exceeds a predefined threshold can obtain the secret.

The main advantage of RRNS is the lower complexity. Operations over interpolation polynomial require a great number of modular multiplications, while in RRNS, there are fast methods of forwarding and backward conversion. It is popular due to a high degree of security. To recover the secret, exactly k shares are required. So that only predefined coalitions (authorized coalitions) unambiguously recover the secret information.

The secret is decomposed into a set of smaller encrypted parts (shares). However, in WA-RRNS system, unlike common SSS based on RRNS, each CSP has several smaller shares. In the following approach allows reducing the probability of information loss at the expense of the reduced speed of coding/decoding.
Let us introduce the following notations.
N number of CSPs
K number of available CSP at a given time
$n_i \geq 1$ number of shares stored in the i-th CSP
Pr(D) probability of denial of access
$\sum_{i=1}^{n} n_i$ number of RRNS moduli
$k \leq n$ threshold value for secret sharing scheme
$r = n-k$ number of control (redundant) RRNS moduli
p RRNS modulus.
In RRNS, the reliability of the system depends on the parameters % and &. Their appropriate selection provides the necessary level of computational security and confidentiality.

$$n = \sum_{i=1}^{N} n_i < \frac{l \cdot 2^{l-1} - 2^l}{l^2}.$$

IV. CONCLUSIONS

In this paper, an identity-based data integrity auditing scheme for secure cloud storage, which supports data sharing with sensitive information hiding. In this scheme, the file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Besides, the remote data integrity auditing remains ready to be efficiently executed. The security proof and therefore the proposed scheme achieves desirable security and efficiency. To reduce the problem of security and reliability issues during a cloud a storage system called RRNS that mixes weighted access scheme and threshold secret sharing redundant residue system with multiple failure detection/recovery mechanisms and homomorphic ciphers. A reliability of the WA-RRNS scheme against known weighted secret sharing schemes. It is clear that although the use of cloud computing has swiftly increased, cloud computing security is still considered the main concern in the cloud computing atmosphere. Customers do not want to lose their secretive information as an outcome of malicious present in the cloud.

REFERENCES

[1] Wenting Shen,Jia Yu,,Rong Hao and Jiankun Hu "Enabling Identity Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage", IEEE transactions on Information Forensics and Security 2018.

[2] Anderi Tehemykh, Mikhail Babenko, Vanessa Miranda- Lopez, Alexander Yu Drozdov, Arutyum Avestisyan "WA-RRNS: Reliable Data Storage System", IEEE International Parallel and Distributed Processing Symposium 2018.

[3] Mohammad Aazam, Eui Nam Huh "Inter cloud Architecture and Media Cloud Storage", International Conference on Cloud Computing 2018.

[4] H. Shacham and B. Waters, "Compact proofs of retrievability", J. Cryptology, Vol- 26, no: 3, pp: 442-483, Jul 2013.

[5] Wang, S. S. M. Chow, Q. Wang, K. Ren and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers, Vol- 62, no: 2, pp: 362-375, 2013.

[6] S. G. Worku, C. Xu, J. Zhao and X. He, "Secure and Efficient Privacy Preserving Public Auditing Scheme for Cloud Storage", Comput. Electr. Eng, Vol- 40, no: 5, pp: 1703-1713, July 2014.

