OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

ACHIEVING PRIVACY OF BIG DATA IN MOBILE CLOUD USING ENCRYPTION TECHNIQUE

Saudagar Nisha Farheen

PG Student, Computer Science & Engineering Department, EESGOI, Aurangabad

---

Abstract: Technology is enhancing each and every day especially in the field of Information Technology and data is very momentous elements. Due to the reasons such as the rapid growth and spread of network services, mobile devices, and online users on the Internet leading to a remarkable increase in the amount of data. Almost every industry is trying to cope with this huge data. Big data phenomenon has begun to gain importance. However, it is not only very difficult to store big data and analyse them with traditional applications, but also it has challenging privacy and security problems. So we proposed system will classify the files in two main categories i.e. Hot files and Cold files. To avoid bottleneck at server end the replicas of hot file will created and stored on different servers. This accession is drafted to magnify privacy protection scope within liquid ate time constraints. Proposed approach aims to selectively encrypt data and use privacy classification methods under timing constraints.

----------∴∴∴----------

I INTRODUCTION

Big data is a high volume, and/or high velocity, high variety information asset, which requires new forms of processing to enable enhanced decision making, insight discovery, and process optimization. Di-vision and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In this project, DROPS methodology, divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Data access control is a challenging issue in public cloud storage systems. Cipher text-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. Clients might be stuck in the sitting tight line for a long stretch to get their mystery keys, along these lines bringing about low-proficiency of the framework.

In spite of the fact that multi expert access control plans have been proposed, these plans still can't conquer the disadvantages of single-point bottleneck and low effectiveness; because of the way that each of the specialists still autonomously deals with a disjoint characteristic set.

We propose a novel heterogeneous framework to remove the problem of single-point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism. Our system utilizes various credit experts to share the heap of client authenticity check. In the interim, in our plan, a CA (Central Authority) is acquainted with create mystery keys for authenticity checked clients. Not at all like other multi specialist get to control plots, each of the experts in our plan deals with the entire quality set exclusively. To enhance security, we also propose an auditing mechanism to detect which AA (Attribute Authority) has incorrectly or maliciously performed the legitimacy verification procedure. Examination demonstrates that our framework ensures the security necessities as well as makes awesome execution change on key generation. Secret sharing is another powerful technique to protect the big data in cloud storage.

The most related work to our proposed scheme are and, whose verification procedure can resist potential attacks such as collusion and cheating. In, two schemes were proposed, namely Scheme-I and Scheme-II, based on the homogeneous linear recursion and the RSA cryptosystem, in

which the homogeneous linear recursion is used to construct the secret share and reconstruct the secret, and RSA is used to verify the users access legitimacy.

The difference between these two schemes lies in that the users in Scheme-I mutually verify each others legitimacy without seeking help from public values while in Scheme-II the users need the help of public values. In [14], the authors presented a verifiable multi-secret sharing scheme based on cellular automata, which is used to construct the secret share and reconstruct the secret with a linear computational complexity, and the RSA cryptosystem, which is used for verification. In these schemes, as multiple users mutually verify each other using multiple RSA operations, a very high computational overhead occurs. In addition, the classic asymmetric crypto solutions would be broken by quantum computing; that is, these traditional verification methods cannot satisfy the verification requirements with respect to quantum computing, which is made closer to reality by IBM in 2015. Thus we need to seek new verification methods to meet the future requirements. For this purpose, we utilize the NTRU cryptosystem to counter the quantum computing attacks in the design of our proposed scheme. Due to the complexity and volume, outsourcing cipher texts 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 cipher text 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; but in practice, access policy update is important for enhancing security and dealing with the dynamism caused by user join and leave activities. In this paper, we propose a secure and veriable access control scheme based on the NTRU cryptosystem for big data storage in clouds. We rst 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. It also enables (i) the data owner and eligible users to effectively verify the legitimacy of a user for accessing the data, and (ii) a user to validate the information provided by other users for correct plaintext recovery. Rigorous analysis indicates that our scheme can prevent eligible users from cheating and resist various attacks such as the collusion attack.

MOTIVATION

The motivation of the proposed system is, companies and organizations are facing a challenging problem of effectively managing their complex data. As the development of cloud storage, outsourcing the data to a cloud is an appropriate approach. Generally speaking, clouds can be classified into two major categories: 1) public clouds with each being a multi-tenant environment shared with a number of other tenants, and 2) private clouds with each being a single-tenant environment dedicated to a single tenant. For example, the IBM cloud was proposed as a public one for the data management of banking.

II LITERATURE SURVEY

1. Yingjie Xue, Jianan Hong,Wei Li and Kaiping Xue, "LABAC: A location aware ttribute-based access control scheme for cloud storage", 2016 IEEE Data access control is a challenging issue in cloud storage.

Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a potential cryptographic technique to address the above issue, which is able to enforce data access control based on users permanent characteristics. However, in some scenarios, access policies are associated with users temporary conditions (such as access time and location) as well as their permanent ones. CP-ABE cannot deal with such situations commendably. In this paper, we focus on the scenario where users access privilege is determined by their attributes, together with their locations. To cope with this data access control requirement, we propose a location-aware attribute-based access control mechanism (LABAC) for cloud. In LABAC, we uniquely integrate CP-ABE with location trapdoors to make up access policies. In this way, data owners can flexibly combine both users attributes and locations to implement a fine-grained control of their data. A competitive advantage of LABAC is that it requires no any additional revocation mechanisms to revoke location-aware access privilege when user location changes. Security and performance analysis are presented which show the security and efficiency of LABAC for practical implementations [4].

2. Zhangjie Fu, Xingming Sun and Sai Ji, "Towards efficient content-aware search over encrypted outsourced data in cloud", IEEE INFOCOM 2016

With the increasing adoption of cloud computing, a growing number of users outsource their datasets into cloud. The datasets usually are encrypted before outsourcing to preserve the privacy. However, the common practice of encryption makes the effective utilization difficult, for example, search the given keywords in the encrypted datasets. Many schemes are proposed to make encrypted data searchable based on keywords. However, keyword-based search schemes ignore the semantic representation information of users retrieval, and cannot completely meet with users search intention. Therefore, how to design a content-based search scheme and make semantic search more effective and context-aware is a difficult challenge. In this

paper, we proposed an innovative semantic search scheme based on the concept hierarchy and the semantic relationship between concepts in the encrypted datasets. More specifically, our scheme first indexes the documents and builds trapdoor based on the concept hierarchy. To further improve the search efficiency, we utilize a tree-based index structure to organize all the document index vectors. Our experiment results based on the real world datasets show the scheme is more efficient than previous scheme. We also study the threat model of our approach and prove it does not introduce any security risk [2].

3. Gaoqiang Zhuo, Qi Jia, "Privacy-preserving Verifiable Set Operation in Big Data for Cloud-assisted Mobile Crowd sourcing", 2017

In this paper, we propose a scheme to enable the requester to delegate set operations over crowd sourced big data to the cloud. Meanwhile, workers data and identity privacy are preserved, and the requester can verify the correctness of the set operation result. We extend our scheme to achieve data preprocessing, batch verification and data update are also proposed to reduce computational costs of the system

4. Dr. S. Prayla Shyry, "A SECURE AND VERIFIABLE ACCESS CONTROL SCHEME FOR BIG DATA STORAGE IN CLOUDS", 2016

Because of the intricacy and volume, outsourcing ciphertexts to a cloud is considered to be a standout amongst the best methodologies for enormous information stockpiling and access. By and by, confirming the entrance authenticity of a client and safely refreshing a ciphertext in the cloud in view of another entrance strategy assigned by the information proprietor are two basic difficulties to make cloud-based huge information stockpiling commonsense and successful. Conventional methodologies either totally disregard the issue of access arrangement refresh or designate the refresh to an outsider specialist yet practically speaking, get to approach refresh is vital for improving security and managing the dynamism caused by client join and leave exercises. In this paper, we propose a safe and evident access control plot in light of the NTRU cryptosystem for huge information stockpiling in mists. We initially propose another NTRU decoding calculation to conquer the unscrambling disappointments of the first NTRU, and afterward detail our plan and break down its rightness, security qualities, and computational proficiency. Our plan enables the cloud server to effectively refresh the ciphertext when another entrance approach is determined by the information proprietor, who is additionally ready to approve the refresh to counter against bamboozling practices of the cloud. It likewise empowers (I) the information proprietor and qualified clients to adequately confirm the authenticity of a client for getting to the information, and (ii) a client to approve the data gave by different clients to revise plaintext
recuperation

III SYSTEM DESIGN

The cloud server to efficiently update the cipher text 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. It also enables (1) the data owner and eligible users to effectively verify the legitimacy of a user for accessing the data, and (2) a user to validate the information provided by other users for correct plaintext recovery. The cloud server can directly update the stored ciphertext without decryption based on the new access policy specified by the data owner, who is able to validate the update at the cloud. The proposed scheme can verify the shared secret information to prevent users from cheating and can counter various attacks such as the collusion attack. It is also deemed to be secure with respect to quantum computing attacks dueto NTRU. When a bank stores its data in the could server only its legal staff members have the rights to access the stored data. Typically the bank system contains many sensitive and private consumer information. In order to reduce the risk of information leakage, the access right of an employee should be properly restricted, and a single employee should not be allowed to reveal the data by itself without obtaining the authorization from other users; that is, recovering the data requires to get the authorization of multiple employees. Moreover, the bank should be able to update the access policies for the stored data in a dynamic and efficient manner. Similarly, military applications can utilize a private cloud to store their complex data. Since the data is confidential, a military member, who needs to access the data, must pass the verification of its legitimacy and receive the authorization from multiple relevant departments. Besides, the military should be able to dyamically and efficiently update its access polices based on the changing requirements.

IV SYSTEM ARCHITECTURE

In this project we propose a secure and verifiable access control scheme for big data storage to tackle the following challenges: i) how to securely store the data in a cloud server and distribute the shares of the access right to all legitimate users of the data? ii) how to verify the legitimacy of a user for accessing the data? iii) how to recover the plaintext data when the access right needs to be jointly granted by multiple users? and iv) how to dynamically and efficiently update the ciphertext in the cloud when the access policy of the data is changed by the data owner To overcome these challenges, we make use of the following techniques in the design of our secure and verifiable access control scheme for big data storage. Typically the bank system contains many sensitive and private consumer information. In order to

reduce the risk of information leakage, the access right of an employee should be properly restricted, and a single employee should not be allowed to reveal the data by itself without obtaining the authorization from other users that is,recovering the data requires to get the authorization of multiple employees. Moreover, the bank should be able to update the access policies for the stored data in a dynamic and efficient manner. Similarly, military applications can utilize a private cloud to store their complex data. Since the data is confidential, a military member, who needs to access the data, must pass the verification of its legitimacy and receive the authorization from multiple relevant departments. Besides, the military should be able to dynamically and efficiently update its access polices based on the changing requirements. Such applications usually require the data to be stored in a cloud in ciphertext format, and the access of the data by a user requires multiple other users to verify the access legitimacy of the user.

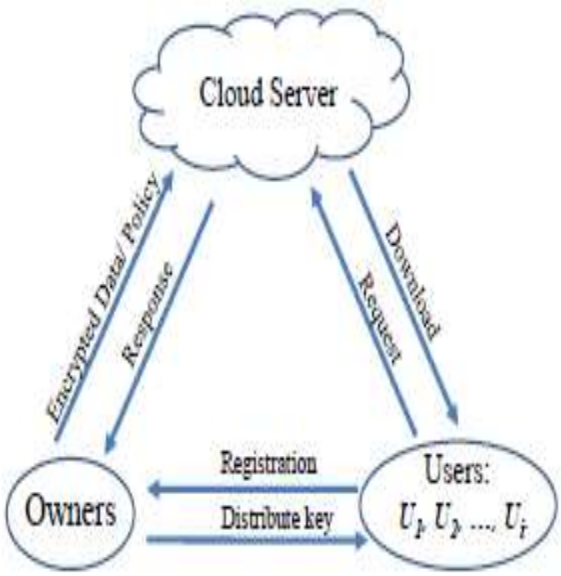

Figure 1: Architecture Diagram

RESULTS

Figure 2: Registration Form

Figure 3: Download uploaded document

Figure 4: Upload File

V CONCLUSION

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 cipher-text to enable efficient access control over the big ata in the cloud.

REFERENCES

[1] Zhangjie Fu, Xingming Sun and Sai Ji, "Towards efficient content-aware search over encrypted outsourced data in cloud", IEEE INFOCOM 2016.

[2] Yingjie Xue, Jianan Hong, Wei Li and Kaiping Xue, "LABAC: A locationaware attribute-based access control scheme for cloud storage", IEEE, 2016.

[3] Gaoqiang Zhuo, Qi Jia, "Privacy-preserving Verifiable Set Operation in Big Data for Cloud-assisted Mobile Crowd sourcing", 2017.

[4] Dr. S. Prayla Shyry, "A SECURE AND VERIFIABLE ACCESS CONTROL SCHEME FOR BIG DATA STORAGE IN CLOUDS".

[5] T. Mohana Priya1 Dr, A.Saradha, R.Rajeshkanna,"An Certain investigations of Emerging Big Data Technologies and its Applications", 2016.

[6] "A Secure and Scalable Data Communication Scheme in Smart Grids", 2016.

[7] A. Corcoles, E. Magesan, S. J. Srinivasan, A. W. Cross, M. Steffen, J. M. Gambetta, and J. M. Chow, "Demonstration of a quantum error detection code using a square lattice of four superconducting qubits", Nature communications, vol. 6, 2015.
[8] O. Regev, "New lattice-based cryptographic constructions", Journal of the ACM (JACM), vol. 51, no. 6, pp. 899942, 2004.
[9] D. Micciancio, "Lattice-based cryptography", in Post-Quantum Cryptography Springer, 2009.
[10] C. Peikert, "Lattice cryptography for the internet", in Post-Quantum Cryptography. Springer, 2014.
[11] J. Hoffstein, J. Pipher, and J. Silverman, "NTRU: Aring-based public key crypto system", in Algorithmic number theory: third international symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998: proceedings, vol. 1423. Springer Verlag, 1998, pp. 267288.
[12] N. Cryptosystems, "The NTRU public key cryptosystem-a tutorial", 1998.
[13] A. Langlois, D. Stehle, and R. Steinfeld, "Gghlite: More efcient multilinear maps from ideal lattices", in Advances in Cryptology EUROCRYPT 2014. Springer, 2014.
[14] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices", in Eurocrypt, vol. 7881. Springer, 2013.
[15] European Telecommunications Standards Institute, "Quantum safe cryptography and security-an introduction, benets, enablers and challenges", European Telecommunications Standards Institute, White Paper, June 2015.
[16] IBM, "IBM storage solutions for banking", http://www03.ibm.com/systems/storage/solutions/industries/banking.html.
[17] A. Mora, Y. Chen, A. Fuchs, A. Lane, R. Lu, P. Manadhata et al., "Expanded top ten big data security and privacy challenges", Cloud Security Alliance, 2013.
[18] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing", Information Sciences, vol. 258, pp. 371386, 2014.
[19] H. Cheng, C. Rong, K. Hwang, W. Wang, and Y. Li, Secure big data storage and sharing scheme for cloud tenants, China Communications, vol. 12, no. 6, pp. 106115, 2015.
[20] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid", IEEE transactions on cloud computing, vol. 3, no. 2, pp. 233244, 2015.
[21] C. Gentry, "A fully homomorphic encryptions cheme", Ph.D. dissertation, Stanford University, 2009.
[22] S. KamaraandK Lauter, "Crypto graphic cloud storage", International Conference on Financial Cryptography and Data Security. Springer, 2010.
[23] A. Hamlin, N. Schear, E. Shen, M. Varia, S. Yakoubov, and A. Yerukhimovich, "Cryptography for big data security", in Big Data: Storage, Sharing, and Security, F. Hu, Ed. CRCPress, 2016.