ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

A Secure and Verifiable Access Control Scheme Based on the Improved NTRU to Protect the Outsourced Big Data Stored In a Cloud

K RAJENDRA PRASAD[1], THEJASWINI M.S [2]

M.Tech Student, Dept. of CSE, BIT Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India. [1]

Assistant Professor, Dept. of CSE, BIT Institute of Technology, Affiliated to JNTU, Andhra Pradesh, India. [2]

ABSTRACT: Due to its complexity and large volume, managing big data cloud server that has the capabilities of storing big data and processing users' access requests in an efficient manner is very difficult, whenever a data owner outsources its data to a cloud, sensitive information may be disclosed because the cloud server is not trusted, therefore usually the ciphertext of the data is stored in the cloud. But when the data owner designs the new access policy it is difficult to update the ciphertext stored in a cloud and to verify the authenticity of a user who intends to access the data. Some basic approaches are used but they failed in some access policy update or delegate the update to a third party authority. To overcome this problem a secure and verifiable access control scheme based on the NTRU cryptosystem for big data storage in clouds, It also enables (a) the data owner and eligible users to effectively verify the legitimacy of a user for accessing the data, and (b) a user to validate the information provided by other users for correct plaintext recovery.

KEYWORDS: Big Data Storage; Access Control; the NTRU Cryptosystem; Secret Sharing; Access Policy Update; Cloud Computing

I.INTRODUCTION

Big data is a collection of huge amount of large datasets and data volume but traditional management process cannot handle the big data storage, With the growing amount of data, the demand for big data storage increases. By placing the data in the cloud, that data is available to anyone from anywhere. Cloud computing is an emerging service-oriented framework for performing distributed and parallel computing over big data storage. Because of the increasing benefits of cloud computing in terms of cost, storage, and scalability and it is also focused by each data providers and institutions for out sourcing their data from the local servers to remote cloud servers, which has become a common trend. This raised major concerns about data security for cloud data storage and the enthusiasm in provisions of improvising the data consistency and privacy, which is causing the major hurdles towards the adoption of clouds services. Most existing approaches for securing the outsourced big data in clouds are based on either attributed-based encryption (ABE) 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 cryptography such as RSA for users' legitimacy verification, which incur high computational overhead. Moreover, 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. As a data owner typically does not backup its data locally after outsourcing the data to a cloud, it cannot easily manage the data stored in the cloud. Besides, as more and more companies and organizations are using clouds to store their data, it becomes more challenging and critical to deal with the issue of access policy update for enhancing security and dealing with the dynamism caused by the users' join and leave activities. To the best of our knowledge, policy update for outsourced big data storage in clouds has never been considered by the existing research.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

Another challenging issue is how to verify the authentication of the users accessing the outsourced data in clouds. Existing schemes proposed in do not support user eligibility verification. On the other hand, verifiable secret sharing based schemes rely on RSA for access authority verification. As multiple users need to mutually verify each other using multiple RSA operations, such a procedure has a high computational overhead.
The considerations for developing the security services in the cloud are

1) Security. The proposed scheme should be able to defend against various attacks such as the collusion attack. Meanwhile, access policy update should not break the security of the data storage, disclose sensitive information about the data owner, and cause any new security problem.
2) Verification. When a user needs to decrypt a stored ciphertext, its access legitimacy should be verified by other participating users and the secret shares obtained from other users must be validated for correct recovery.
3) Authorization. To reduce the risk of information leakage, a user should obtain authorization from the data owner for accessing the encrypted data.

II. LITERATURE SURVEY

Security is one of the major challenges facing the cloud environment. The 88% of cloud consumers request access to their data and request greater consideration to reverses, such as possible cloud consumers physical location, data management and security administration of their cloud data in virtual environments. This indicates that users recognize clearness and security over cloud information. The service provider may be fully controlled by managing the cloud service of a cloud service, but some cloud service providers do not allow the user to use cloud information in the cloud.

Chi Chen et. al proposes a search mechanism in the ciphertext cloud storage. It explores the difficulty of preserving a semantic association among various simple documents in relation to the encrypted documents and provides a method to improve the performance of the semantic search. The proposed method has an advantage over the conventional method of ranking privacy and the relevance of the retrieved records, as it analyzes search competence and security beneath two admired threat patterns. The work is focused only on data privacy but the effectiveness and accessibility of various search users are not discussed.

Zheng Yan et. al focuses on storing encrypted data with encryption running for "secure", "reliable", and "green cloud storage service", particularly for large data systems.It suggests function based on the encryption name ABE, to copy the encrypted data stored in the cloud as it supports the ability to access data at the same time. Existing solutions to copying are subject to brute attacks and do not support data access control and returns smoothly. It is based project to support encrypted data stored in the cloud at the equivalent time supports protected data access control. This proposal does not evaluate competitive data ownership verification and flexible compensation for supporting copy and data access controlled for schema optimization.

V. Chang et. al proposed a CCAF multi-layer security protects real-time data, and it has three layers of security: 1) "firewall and access control"; 2) "Identification Management and Intervention Prevention", and 3) "Conversion Encryption". It has taken two sets of ethical-hacking experiments in intrigue testing. The CCAF multi-layer security protects data from speedy data expansion because of security violates. This method provides real-time protection for all the data, prevents more threats and removes the systematic system in the data centre and provides a comprehensive explanation of cloud security supported by a comprehensible structure that affects the performance of useraccessed service, business process modelling. It can be further evaluated in real-time scenarios to measure efficiency.

III. EXISTING SYSTEM

Cloud computing offers a new way of service provision by re-arranging various resources over the Internet. The most important and popular cloud service is data storage. In order to preserve the privacy of data holders, data are often stored in cloud in an encrypted form. However, encrypted data introduce new challenges for cloud data de-duplication,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

which becomes crucial for big data storage and processing in cloud. Traditional de-duplication schemes cannot work on encrypted data. Existing solutions of encrypted data de-duplication suffer from security weakness. They cannot flexibly support data access control and revocation. Therefore, few of them can be readily deployed in practice

Disadvantages

- Less Efficiency
- Less Security
- Repeated data Storage unnecessarily

IV.PROPOSED WORK

This project proposes a scheme to reduplicated encrypted data at Cloud Service Provider by applying RNS algorithm to issue keys to different authorized data owners based on data ownership challenge. Data owners are responsible for the file encryption, de-duplication and access control of users. Data owner uploads a file to cloud with de-duplication encryption concept, after uploading based on users attributes, data owner generates key using DES algorithm and will be sent to the authorized user through the mail id. A user has to download the key from mail and if key matches user can download the file.

Advantages

- More SECURITY is given for the files which are outsourced to cloud using RNS Encryption and decryption technique.
- Usage of cloud space efficiency using de-duplication concept.
- High speed of transmission.

V. SYSTEM ARCHITECTURE

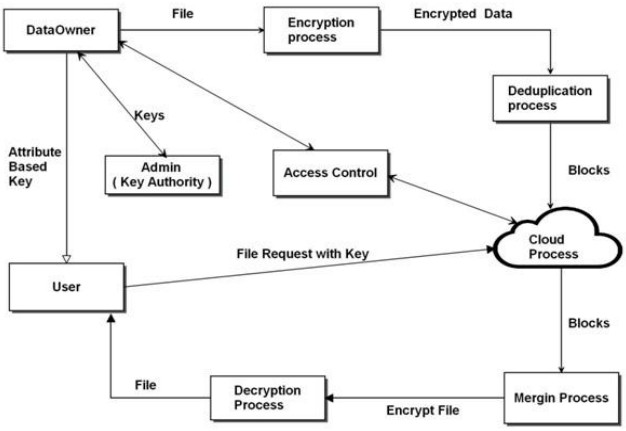

Fig:1 System Architecture.

System architecture describes the overall architecture of the system which contains a Admin, Data Owner and User. These provide a secure and verifiable access control scheme by checking the de-duplication process and also by generating hash code

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

VI. IMPLEMENTATION

1. Data Owner Creation Module

In this module admin going to create data owner with valid details and for every data owner admin going to create encryption and decryption keys using asymmetric algorithm.

2. Key Generation Module

In this module admin going to generate two keys for encryption and decryption process. By using Asymmetric algorithm RNS, admin going to generate master secret key and public key and stored in the server.

3. User Creation and Mail Sending Module

In this module Data owner going to create users, while creating users private key is created for different users, In the private key attribute based information of user and private key of data owner is encrypted with the help of DES algorithm and sent to user mail id using SMTP protocol

4. Upload file using HDFS Module

Data Owner has to select the file from system and click to upload option. Files will get divided into small blocks (500 bytes each block).Generate hash tag for all block. Compare generated hash block with existing hash tag from database if hash tag matched in that case we will not upload that block into Cloud Storage, we will increase number of instance of that block in database table. If hash tag not matched in that case we will add that block hash details in database and upload that block in cloud. LBA - Logical Block Addressing technique is used to identify what are the blocks are present in a file. After uploading file to cloud, give access control to file

5. Download file

User has to give private key which is downloaded from mail id, decrypt the private key using DES algorithm and get the information about attributes of user. If user attributes and file attribute is matched means, all the LBA blocks downloaded from Cloud Storage and merged and decrypted back to original form using RNS Algorithm decryption key and transaction details can be viewed by user.

VII. CONCLUSION

In this paper, an improved framework of 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 is implemented and it the framework also 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. It also provides a verification process for a user to validate its authenticity of accessing the data to both the data owner and other genuine users and the correctness of the information provided by the other users for plaintext recovery.

REFERENCES

[1] M. A. Beyer and D. Laney, "The importance of big data: a definition," Stamford, CT: Gartner, 2012.
[2] V. Marx, "Biology: The big challenges of big data," Nature, vol. 498, no. 7453, pp. 255–260, 2013.
[3] G. P. Consortium et al., "A map of human genome variation from population-scale sequencing," Nature, vol. 467, no. 7319, pp. 1061–1073, 2010.
[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT 2005, pp. 457–473, 2005.
[5] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.
[6] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94–107, 2016.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 89–98.
[8] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," Public Key Cryptography–PKC 2011, pp. 53–70, 2011.
[9] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," IEEE journal on selected areas in communications, vol. 31, no. 9, pp. 37–46, 2013.
[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT 2011, pp. 568–588, 2011.
[11] C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, "An attribute based signcryption scheme to secure attribute-defined multicast communications," in SecureComm 2015. Springer, 2015, pp. 418–435.
[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.
[13] M. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multisecret sharing," Computer Standards & Interfaces, vol. 30, no. 3, pp. 187–190, 2008.
[14] Z. Eslami and J. Z. Ahmadabadi, "A verifiable multi-secret sharing scheme based on cellular automata," Information Sciences, vol. 180, no. 15, pp. 2889–2894, 2010.
[15] M. H. Dehkordi and S. Mashhadi, "New efficient and practical verifiable multi-secret sharing schemes," Information Sciences, vol. 178, no. 9, pp. 2262–2274, 2008.
[16] J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," Computer Standards & Interfaces, vol. 29, no. 1, pp. 138–141, 2007.