Scientific Journal Impact Factor (SJIF): 5.278

International Journal of Modern Trends in Engineering and Research

IJMTER

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

FUZZY IDENTITY AND ATTRIBUTE BASED ENCRYPTION FOR FINE GRAINED ACCESS CONTROL OF ENCRYPTED DATA

K.Meena[1] and S.Abarna[2]

[1]PG Scholar of CSE, Chandy College of Engineering

[2]Assistant Professor of CSE, Chandy College of Engineering

Abstract— 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 ext 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. 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 plain text recovery.

Keywords—Big Data Storage, Access Control, NTRU Cryptosystem, Secret Sharing, Access Policy Update, Cloud Computing

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 [1]. Due to its complexity and large volume, managing big data using on hand database management tools is difficult. An effective solution is to outsource the data to a cloud server that has the capabilities of storing big data and processing users' access requests in an efficient manner. For example in e health applications, the genome information should be securely stored in an e-health cloud as a single sequenced human genome's around 140 gigabytes in size [2]. 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 [3] 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 cipher text. Secret sharing [4] 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.

II. EXISTING SYSTEM

In this information era, 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..When a bank stores its data in the cloud server, only for 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. Such applications usually require the data to be stored in a cloud in cipher text format, and the access of the data by a user requires multiple other users to verify the access legitimacy of the user. Therefore in this paper propose a secure and verifiable access control scheme for big data storage to tackle the following challenges 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? How to verify the legitimacy of a user for accessing the data? How to recover the plaintext data when the access right needs to be jointly granted by multiple users? How to dynamically and efficiently update the cipher text 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. First, a plaintext data is bound to a secret that is shared by all legitimate users of the data based on (t;n)-threshold secret sharing, and a message certificate is computed for the data based on the NTRU encryption; the cipher text is produced from both the shared secret and the message certificate.

III. PROPOSED SYSTEM

In this Proposed System can select NTRU is used for the process. In this process, File can be encrypted with the help of “DES” algorithm. Next process, we can store the encrypt file into CSP. CSP is one of the server which is used for the storage process. This benefit has contributed to its popularity in cryptographic software. Virtual machine can offer an instruction set architecture that differs from real computer's; Easy maintenance, application provisioning, availability and convenient recovery. Finally, the file can be in proper way. Another proposed system is that the system proposes a new cloud storage scheme in proof of retrievable for cloud storage, in which a trustworthy audit server is introduced to preprocess and upload the data on behalf of the clients. On the other side we improve the semi-honest trust worthy and ensure dynamic data process in cloud and this system develops a strengthened security model for considering data security and the storage server in the upload phase of an integrity verification scheme.

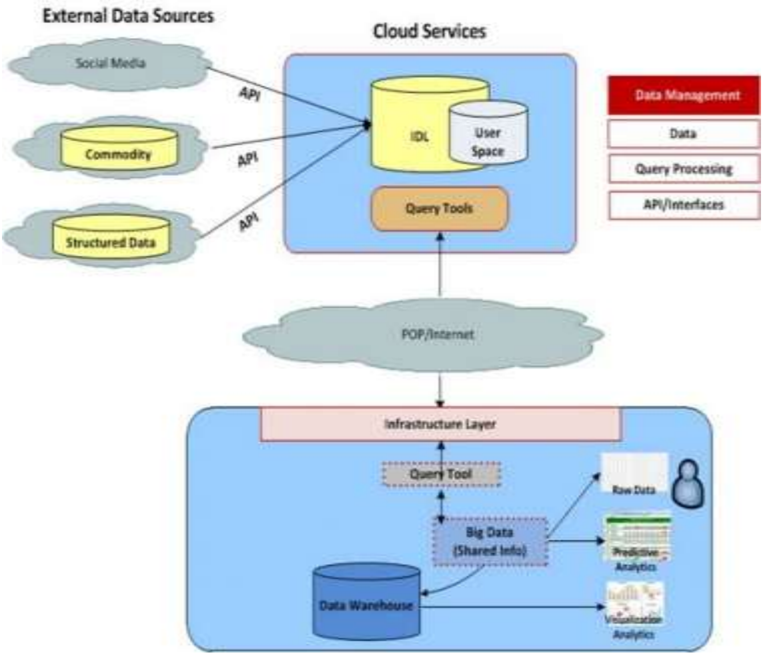

Figure 1. Construction of the proposed system

IV. BLOCK DIAGRAM DESCRIPTION

The block diagram of proposed system contains public clouds with each being a multi-tenant environment shared with a number of other tenants. 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. When a bank stores its data in the server only the 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 dynamically and efficiently update its access polices based on the changing requirements.

V. FLOW DIAGRAM AND DESCRIPTION

In the initial phase, the login process is performed. If the user is new user means, the registration process performed and the user will register their information into the database .Here the user have to create the cloud Id Again the user login process are performed. Content owner have to select the data and the data may be at any format. If the data is in pdf or ppt or doc means that data are converted into text format. Data owner generates the message authentication code for the data. It contains the name of the receivers. Only those authorized users can receive the data from CSP.CSP (Cloud Service Provider) receives the following contents from data owner. They are

i) Encrypted data.
ii) Authorization Rules.
iii) Re-Encryption keys.

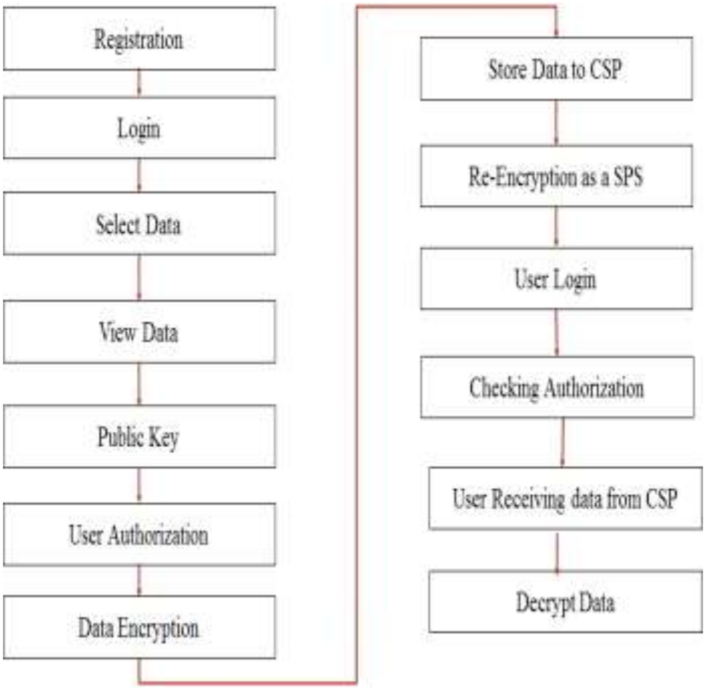

Figure 2. Data Flow Diagram

VI. MODULES DESCRIPTION

A. Initial Phase - In the initial phase, the login process are performed. If the user is new user means, the registration process performed and the user will register their information into the database. The cloud Id has to be created. Again the user login processes are performed. After that the data will be transferred in a proper way.

B. Owner Process - Content owner have to select the data and the data may be at any format. If the data is in pdf or ppt or doc means that data are converted into text format. Then it will be encrypted by the same manner.

C. Encryption Process - Data owner generates the message authentication code for the data. This MAC is used as the key for the encryption of the data. For encryption Data Encryption Standard algorithm (DES) is used. It uses 56 bits as key size. And also the data owner sends the authorization rules. It contains the name of the receivers. Only those authorized users can receive the data from CSP.

D. CSP-SPS - CSP (Cloud Service Provider) receives the following contents from data owner. They are Encrypted data., authorization Rules, Re-Encryption keys. Using the re encryption key the encrypted data have be encrypted again. Then the cloud service provider is ready to provide service to the data user. Cloud service provider receives the request from data user. This re encryption mechanism increases the security of the data.

E. Consumer Process - Data user have to login into the system. and send the request to the cloud service provider. Cloud service provider validates the request from the data user. For this validation process the authorization rules are used. If the data user name is present in the authorization rules means the CSP will provide the data. Otherwise CSP will not provide the data. Then the data user decrypts the data received from the cloud service provider.

VII. CONCLUSION

In this project 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 data in the cloud. It also provides a verification process for a user to validate its legitimacy of accessing the data to both the data owner and other legitimate users and the correctness of the information provided by the other users for plaintext recovery. The security of our proposed scheme is guaranteed by those of the NTRU cryptosystem and the (t;n)-threshold secret sharing.

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] Sahai and B. Waters, “Fuzzy identity-based encryption,” Advances in Cryptology–EUROCRYP 2005, pp. 457–473, 2005.

[5] 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] 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.