Proceedings of Second Shri Chhatrapati Shivaji Maharaj QIP Conference on Engineering Innovations
Organized by Shri Chhatrapati Shivaji Maharaj College of Engineering, Ahmednagar
In Association with Novateur Publications JournalNX-ISSN No: 2581-4230
February, 22nd and 23rd, 2019

A Novel Methodology Used To Store Big Data Securely In Cloud

Kale Piyusha Balasaheb
Dept. Of Computer Engineering
SCSMCOE, Nepti, Ahmednagar
Ahmednagar, India
piyushabkale748@gmail.com

Pawar Shital Vijaykumar
Dept. Of Computer Engineering
SCSMCOE, Nepti, Ahmednagar
Ahmednagar, India
shital33pawar@gmail.com

Ukande Monika Prakash
Dept. Of Computer Engineering
SCSMCOE, Nepti, Ahmednagar
Ahmednagar, India
monikaukande22@gmail.com

Bodkhe Asha Dharmaji
Dept. Of Computer engineering
SCSMCOE, Nepti, Ahmednagar
Ahmednagar, India
asha23bodkhe@gmail.com

Abstract— Big data are voluminous and complex for that retrieving cipher text to a cloud is deemed to be one Of most effective approaches for big data storage and access. The new policies are proposed in cloud where access legitimacy of user and updating cipher text security designated by data owner are two critical challenges to make cloud based data storage practical and effective. Existing approach are completely avoid access policy but in reality it is important to update the access policy amplify the security and dealing with different cause by user join and leave activity. In this system, we plan a secure and verifiable access control scheme based on NTRU cryptosystem for big data storage in cloud. First the new NTRU decryption algorithm meet the decryption fault of the original NTRU, then details of its analyse its correctness, security strength and computational efficiency. When new access policy is specified by big data owner our system allows the cloud server to efficiently update the cipher text. Which is able to update and validate policy against cheating scheme of cloud? It also authorize the end user to validate information by other user for data access and a user to validate the information provided by for recovery of plaintext.

Keywords—NTRU Cryptosystem, Big Data, Cipher Text

I. INTRODUCTION

Enormous information is a high volume, as well as high speed, high assortment data resource, which requires new types of preparing to empower upgraded basic leadership, understanding disclosure, and process improvement. Because of its intricacy and substantial volume, overseeing huge information utilizing close by database administration instruments is troublesome. A viable arrangement is to outsource the information to a cloud server that has the capacities of putting away huge information and handling clients' entrance asks for in a proficient way. For instance in e-health applications, the genome data thought to be safely put away in an e-wellbeing cloud as a solitary sequenced human genome is around 140 gigabytes in measure.

In any case, when an information proprietor outsources its information to a cloud, delicate data might be unveiled on the grounds that the cloud server isn't trusted; Normally the cipher text of the information is put away in the cloud. Be that as it may, how to refresh the ciphertext put away in a cloud when another entrance strategy is assigned by the information proprietor and how to check the authenticity of a client who means to get to the information are still of awesome concerns.

II. GOALS AND OBJECTIVES

- To implement a secure and verifiable access control scheme based on NTRU cryptosystem for big data storage in cloud.
- To reduce the risk of information leakage, a user should obtain authorization from the data owner for accessing the encrypted data
- To update and validate policy against cheating scheme of cloud.
- To defend against various attacks such as the collusion attack.

III. LITERATURE SURVEY

[1]Surajkumar Singh, Niraj Chaudhary, Sreenu M., Manjunath B. M., "Secure Accessibility for Big Data in Cloud", 2018.

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. The security of our proposed scheme is guaranteed by those of the NTRU cryptosystem and the (t,n)-threshold secret sharing. We have rigorously analyzed the correctness, security strength, and computational complexity of our proposed scheme.

[2]Kai Fan, Junxiong Wang, Xin Wang, Hui Li and Yintang Yang, "A Secure and Verifiable Outsourced Access Control Scheme in Fog-Cloud Computing Sensors", 2017.

With the rapid development of big data and Internet of things (IOT), the number of networking devices and data volume is increasing dramatically. Fog computing, which extends cloud computing to the edge of the network can

effectively solve the bottleneck problems of data transmission and data storage. However, security and privacy challenges are also arising in the fog cloud computing environment. Ciphertext-policy attribute-based encryption (CP-ABE) can be adopted to realize data access control in fog-cloud computing systems. In this system, we propose a verifiable outsourced multi-authority access control scheme, named VO-MAACS. In our construction, most encryption and decryption computations are outsourced to fog devices and the computation results can be verified by using our verification method. Meanwhile, to address the revocation issue, we design an efficient user and attribute revocation method for it. Finally, analysis and simulation results show that our scheme is both secure and highly efficient.

[3]Roslin Dayana K., Vigilson Prem M., "Review of the Various Optimized Access Control Techniques for Big Data in Cloud Environment", 2018.

Cloud computing is an information technology (IT) domain that enables efficient access to shared and private collection of configurable system resources. It provides higher-level services that can be very quickly provisioned at a greater rate with minimum amount of effort for management, mostly over the Internet. Due to the high complexity and huge volume, outsourcing ciphertexts to a cloud is deemed to be one of the most effective approaches for big data storage and access. Verifying the access legitimacy of a user and securely updating a ciphertext in the cloud based on a new access policy designated by the data owner are two critical challenges. The access policy update is important for enhancing security and dealing with the dynamism caused by user joins and leave activities. In this paper, the two different approaches developed recently to provide the secure, verifiable and flexible access control of Big data storage in cloud are discussed to solve the above challenges.

[4]Dr. S. Prayla Shyry, Dhrupad Kumar Das, "A Secure And verifiable Access Control Scheme for Big Data Storage in Clouds".

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.

IV. MOTIVATION

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. Generally speaking, clouds can be classified into two major categories: i) public clouds with each being a multi-tenant environment shared with a number of other tenants, and ii) private clouds with each being a single-tenant environment dedicated to a single tenant. In this system 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 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. 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 ciphertext is produced from both the shared secret and the message certificate.

V. PROPOSED SYSTEM

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 framework employs multiple attribute authorities to share the load of user legitimacy verification. Meanwhile, in our scheme, a CA (Central Authority) is introduced to generate secret keys for legitimacy verified users. Unlike other multi- authority access control schemes, each of the authorities in our scheme manages the whole attribute set individually.

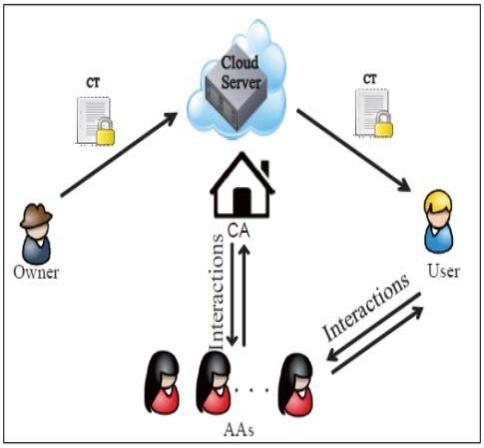

Fig 1: System Architecture

To enhance security, we also propose an auditing mechanism to detect which AA (Attribute Authority) has incorrectly or maliciously performed the legitimacy verification procedure. Analysis shows that our system not only guarantees the security requirements but also makes great performance improvement on key generation.

VI. IMPLEMENTATION MODULES

The system model of our design is shown in Fig. which involves five entities: a central authority (CA), multiple attribute authorities (AAs), many data owners (Owners), many data consumers (Users), and a cloud service provider with multiple cloud servers(here, we mention it as cloud server.).

A. The central authority (CA): CA is the administrator of the entire system. It is responsible for the system construction by setting up the system parameters and generating public key for each attribute of the universal attribute set. In the system initialization phase, it assigns each user a unique Uid and each attribute authority a unique Aid. For a key request from a user, CA is responsible for generating secret keys for the user on the basis of the received intermediate key associated with the users legitimate attributes verified by an AA. As an administrator of the entire system, CA has the capacity to trace which AA has incorrectly or maliciously verified a user and has granted illegitimate attribute sets.

B. The attribute authorities (AAs): AAs are responsible for performing user legitimacy verification and generating intermediate keys for legitimacy verified users. Unlike most of the existing multi-authority schemes where each AA manages a disjoint attribute set respectively, our proposed scheme involves multiple authorities to share the responsibility of user legitimacy verification and each AA can perform this process for any user independently. When an
AA is selected, it will verify the users legitimate attributes by manual labor or authentication protocols, and generate an intermediate key associated with the attributes that it has legitimacy-verified. Intermediate key is a new concept to assist CA to generate keys.

C. The data owner (Owner): Data owner defines the access policy about who can get access to each file, and encrypts the file under the defined policy. First of all, each owner encrypts his/her data with a symmetric encryption algorithm. Then, the owner formulates access policy over an attribute set and encrypts the symmetric key under the policy according to public keys obtained from CA. After that, the owner sends the whole encrypted data and the encrypted symmetric key (denoted as ciphertext CT) to the cloud server to be stored in the cloud.

D. The data consumer (User): User is assigned a global user identity Uid by CA. The user possesses a set of attributes and is equipped with a secret key associated with his/her attribute set. The user can freely get any interested encrypted data from the cloud server. However, the user can decrypt the encrypted data if and only if his/her attribute set satisfies the access policy embedded in the encrypted data.

E. The cloud server : Cloud Server provides a public platform for owners to store and share their encrypted data. The cloud server doesnt conduct data access control for owners. The encrypted data stored in the cloud server can be downloaded freely by any user.

VII. ALGORITHM

A Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme consists of four algorithms.

1. Setup(λ ,U) (PK,MSK). The setup algorithm takes the security parameter and the attribute universe description U as the input. It outputs the public parameters PK and a master secret key MSK

2. Encrypt(PK,M,A) CT. The encryption algorithm takes the public parameters PK, a message M, and an access structure A as input. The algorithm will encrypt M and produce a ciphertext CT such that only a user whose attributes satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.

3. Key Gen(MSK, S) SK. The key generation algorithm takes the master secret key MSK and a set of attributes S as input. It outputs a secret key SK.

4. Decrypt(PK,CT, SK) M. The decryption algorithm takes the public parameters PK, a cipher text CT which contains an access policy A, and a secret key SK as input, where SK is a secret key for a set S of attributes. If the set S of attributes satisfies the access structure A, the algorithm will decrypt the cipher text and return a message M.

VIII. MATHEMATICAL MODEL

Let,

S = {R, T, D}

R = Registration of the file owner on cloud.

T = Validate data user and forward report to system CA

O = Observe CA

D=Send Decryption key on registered email

R = {r0, r1, r2, r3}

Where,

r0 = Provide information to the registration authority

r1 = Registration authority validate the information

r2 = owner get cloud id and owner id

r3 = after verification owner upload data to the cloud

r3 → o0

O = {o0, o1, o2}

Where,

o0 - CA will be chosen among AAs

o1 - Observer will observe CA for its behavior if any discrepancy found creates report

o2 - On report generation, change CA among AAs.

o0 → t0

IX. RESULTS

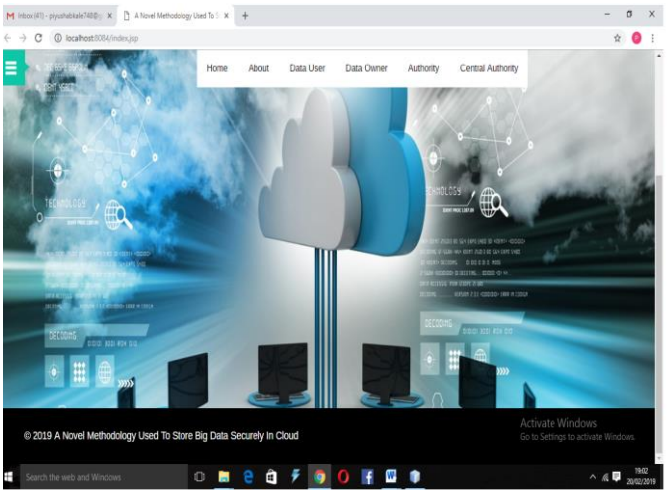

Fig 2: Home Page

Fig 3: User Registration

Fig 4: User Login

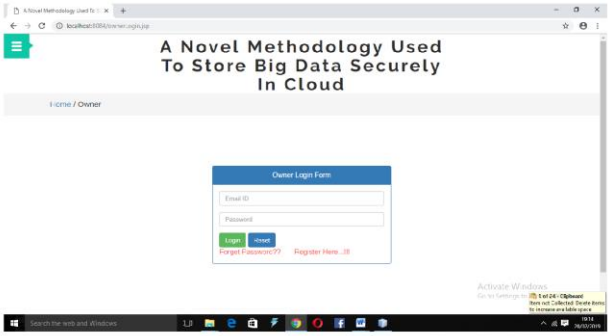

Fig 5: Owner Login

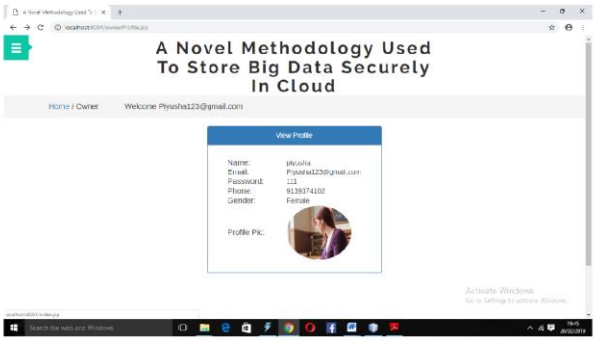

Fig 6: View Profile

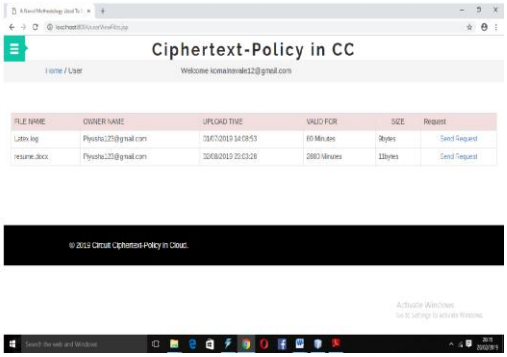

Fig 7: Access File

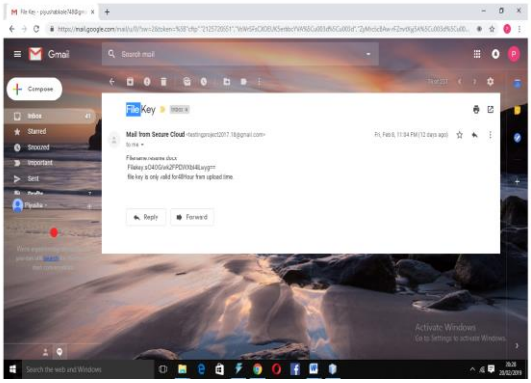

Fig 8: Encrypted Key From System

X. CONCLUSION

In this system, 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 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 legitimacy of accessing the data to both the data owner and t-1 other legitimate users and the correctness of the information provided by the t-1 other users for plaintext recovery.

ACKNOWLEDGMENT

We express our sincere thanks to our project guide Prof. Lagad J. U. who always being with presence & constant, constructive criticism to made this paper. We would also like to thank all the staff of COMPUTER DEPARTMENT for their valuable guidance, suggestion and support through the project work, who has given co-operation for the project with personal attention. Above all we express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during project work. At the last we thankful to our friends,

colleagues for the inspirational help provided to us through a project work.

REFERENCES

[1]Surajkumar Singh, Niraj Chaudhary, Sreenu M., Manjunath B. M., "Secure Accessibility for Big Data in Cloud", 2018.

[2]Kai Fan, Junxiong Wang, Xin Wang, Hui Li and Yintang Yang, "A Secure and Verifiable Outsourced Access Control Scheme in Fog-Cloud Computing Sensors", 2017.

[3]Roslin Dayana K., Vigilson Prem M., "Review of the Various Optimized Access Control Techniques for Big Data in Cloud Environment", 2018.

[4]Dr. S. Prayla Shyry, Dhrupad Kumar Das, "A Secure And verifiable Access Control Scheme for Big Data Storage in Clouds".

[5] Chunqiang Hu, Wei Li, Xiuzhen Cheng, Jiguo Yu, Shenling Wang, Rongfang Bie, "A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud", IEEE Transactions on Big Data, Vol pp, Issue 99, Feb 2017.

[6] Zheng Yan, Xueyun Li, Mingjun Wang, Athanasios V. Vasilakos, "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing", IEEE Transactions on Cloud Computing, Vol. 5, Issue 3, July-Sept. 1 2017.

[7] E. Goh, H. Shacham, N. Modadugu, D. Boneh, Sirius: Securing untrusted storage, Proc. of NDSS, 2003, pp. 131145.

[8] L. Zhou, V. Varadharajan, M. Hitchens, Achieving secure role-based access control on encrypted data in cloud storage, IEEE Trans. on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, 2013.

[9] C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, An attributebased signcryption scheme to secure attribute-defined multicast communications, in SecureComm 2015. Springer, 2015, pp. 418435.

[10] M. Dehkordi and S. Mashhadi, An efficient threshold verifiable multisecret sharing, Computer Standards Interfaces, vol. 30, no. 3, pp. 187190, 2008. SCSM COE, Department of Computer Engineering 2018-19 46.