IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

High Secure and dynamic Access Control Scheme for Big Data Storage in Cloud Environment

P. Jayasree[1]*, V. Saravanan[2]

[1]Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, India
[2]Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, India

*Corresponding Author: kandasamysree@gmail.com, Tel.: +91-9943799375

Available online at: www.ijcseonline.org

Accepted: 12/Jul/2018, Published: 31/Jul/2018

Abstract: Data storing and sharing becomes a most important exceptionally attractive service supplied by cloud computing platforms because of its convenience cost effective platform and more economy. Data owner to store and outsourcing their data in the cloud and through which provide the data access to the user However, outsourcing data to a third-party administrative control entails serious security concerns. Cloud client upload Data leakage may be occur due to attacks by other users and machines in the cloud. Data leakage is and data privacy strategies an ongoing problem in the field of cloud security. The proposed work identifies security and privacy issues for secure data management in cloud environment. The proposed system provides a novel effective scheme that is named as HSDS-DP (High Secure Data Share with dynamic policy update), which is a new technique for data privacy with improved security features. The proposal has three main contributions such as, Threshold Secret Sharing, Dynamic access control update, and key managers. The proposed method Client receives public keys from all Key Managers (KM), afterwards client generate random symmetric-key for perform encryption, Symmetric key are protected by the public key. Encrypted data and keys are uploaded in the cloud. For accessing the file client should download encrypted entire key share and encrypted data file from cloud. Accessing the data client send share of key to the Key Managers, so that client will receives backs decrypted share. Proposed Dynamic Access Policy Update Scheme so client dynamically updates the data access making request to cloud server. The results reveal that proposed can be effectively used for security of outsourced data by employing key management, access control, and file dynamic access policy updating process. Our proposed scheme can prevent cheating and Data leakage problem in public cloud infrastructure.

Keywords: Data security**,** Access Control, Secret Sharing, Cloud computing, Semi-Trusted Third Party, key management

I. INTRODUCTION

Cloud computing has been emerged with upcoming technologies which plays a vital role in developing IT industry. Cloud has been ventured the services with the promise to satisfy the business needs. This has resulted in cost reduction and also convolution involved in owning and operating computers and network.

Cloud computing results to be excellent in case of data storage meanwhile problems arise at the time of annihilating the security. As technology grows, mechanisms for threatening the data storage have been increased [1]. Therefore, cloud users concerns regarding their data security.

Data security is all about the integrity of data, availability of data, confidentiality. Meanwhile un trusted servers to ensure the integrity of data is a big anxiety for the users. Intruder refers to the unauthorized users who can miss use the data of the user. Maintaining accuracy and consistency Comes under the data integrity. Maintaining secrecy of the data refers to the confidentiality of data; while is a protocol for maintaining those information. It's is necessary that the user shouldn't share any information related to anybody [2]. Major Data Access Control is Dac, Mandatory Access Control, RBAC, etc. Authorized users ensure to access the information [3].

Section I contains the introduction of the Paper regarding the Secure storage of data in Cloud , Section II contain the related work of problem done in previous methods , Section III contain the some measures of proposed methodology High Secure and dynamic Access Control Scheme for Big Data Storage. Section IV contain the implementation of HSDS-DP algorithm, section V explain the experimental results of HSDS-DP, Section VI concludes research work with future directions.

II. PROBLEM DEFINITION

The cloud data security is widely used by many researches. But only few approaches were concentrated on the cloud data security and access control on cloud services. Because big data frequently contains a huge amount of personal identifiable information, how to securely store the data and how to provide access control over the stored data are two biggest challenges.

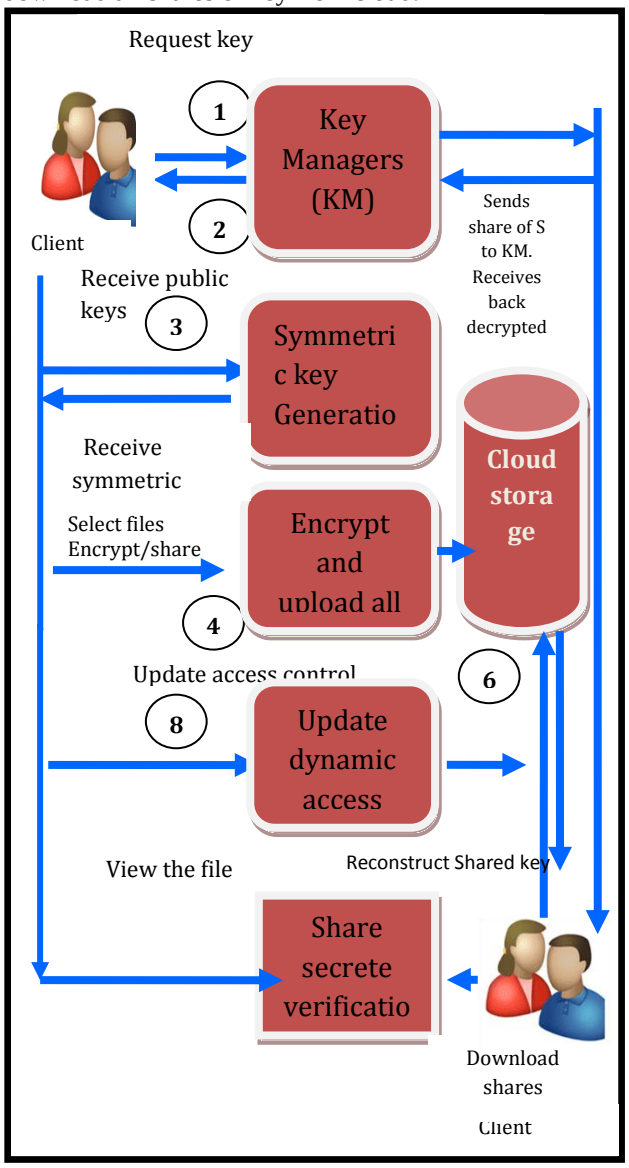
Data Loss is an important threat in cloud computing. Losing data due to a malicious attack and sometimes due to server crashes or deletion by the provider without having backups. Manage the data stored in the cloud its more tedious task [4], [5]. When a data owner outsources or upload its most important data to a cloud, This Sensitive information may be disclosed because the cloud server is not trusted services. Access control is key to protect the stored data. In which the data owners define the access policies based on the attributes [6]. By this way the data owners are able to ensure that only the users who are all meeting the access policies can view the cloud uploaded data However, change the access control in cloud servers, and update dynamic data access control becomes a challenging issue in cloud storage[7],[8].

III. PROPOSED SYSTEM

Cloud data security is focused on the proposed work. In the proposed system, HSDS-DP (High Secure Data Share with dynamic policy update) is presented. In case of data protection access control to the data is a primary concern. Authorized users have the full rights to access the data requested in the cloud. The proposed system access the TSSD technique, which poses the threshold key share and so provides security for cloud data. This enhances the security mechanisms for those who are accessing the data. This chapter discusses the overview of proposed system, the process along with the function involved. The proposed TSSD technique can be classified as,

- Key Generation/Data encryption
- Threshold Secret Sharing
- Share secret verification
- Dynamic access control

The data owner or client will send a request to all Key Managers (KM), as soon as the key managers receives the request, will forward the public keys for those who are requested clients. While receiving the public key from the key manager, client will generate random symmetric key in order to carry out the encryption process. Symmetric keys are protected by the public key, which regenerated by the key manager. Client after successfully receive the public key and secret key, then client can encrypt upload a text document in the cloud storage with the accessibility specification .The access specification is nothing but specifying control for over the document which means matched user can able to view and access the document Client Upload all shares to cloud. For accessing the cloud file initially Client needs to download all shares of key from cloud.



The following fig 1.0 represents the overall process of the proposed in TSSD scheme. After successful of share download client Sends share to Key manager then client will be Receives back decrypted share. In order to decrypt the cipher texts the user's eligibility must be verified by at least Threshold value other user for reconstruct the secret. After successful of secrete re-construction only user can able to get and view the cloud file information. Client can dynamically changes the access right to particular upload document .For change the access control client has to send query process to cloud server. So that server will dynamically and efficiently update the access control of the data.

METHODOLOGIES IN THE PROPOSED SYSTEM

The followings are the main contribution of the proposed system

1. Improved NTRU
2. Threshold Secret Sharing
3. Dynamic Access Policy Update Scheme.

A) **Improved NTRU**

The first contribution of the proposed system is the creation of public key. Improved NTRU is the first public key cryptosystem not based on factorization.

Algorithm: Improved NTRU

Step 1: Encryption

Read the content from a file and store in string builder.

Convert the string builder in to character array.
Take every character from an array then take its ASCII value after that convert it in binary value 10011101111110000001.

Step 2: randomly chooses 2 small polynomials f and g
f (x) = x^6−x^4+x^3+x^2−1
g(x) = x^6+x^4−x^2−x
Step 3: Find N such that N = F G

N will be used as the modulus for both the public and private keys

Find the totient of n, ϕ(n) ϕ(n)=(f-1)(g-1)

Step 4: e = n*f +m (modulo q),

e is encrypted message, m is plaintext, f is public key

Step 5: Take the decryption files from computer and read its content.

Step 6: strings from file then store in string builder then convert that string in to char array then take every character and store that character as ASCII value in array list then get binary value from array list.

Step 7: N will be used as the modulus for both the private key

Find the totient of n, ϕ(n) ϕ(n)=(f-1)(g-1)

Step 8: d = n*fg+e (modulo q),

d is decrypted message, m is encrypted text, f is private key

Initially client has to select the file and make a encryption process. Encryption of the file uploaded by the client with help of Improved NTRU encryption /decryption algorithm. This algorithm more efficient encryption and decryption
This performs much faster key generation process.

B). Threshold Secret Sharing

Algorithm Threshold Secret Sharing

Step 1: Secret key spilt in to N number of Pieces

Step 2: Set the thresh hold for share

Step 3: Encrypts i-th share with public key of i-th KM

Step 4: Share the spilt secret to cloud

Step 5: Selects k number of KMs randomly. Sends i-th share of S to i-th KM

Step 6: Get decrypted i-th share

Step 7: Reconstruct and Apply the collect share Secret key and system will check thresh hold level.

Step 8 display the file content

Steps for dynamic policy update

Step 1: Select the user upload file {f1, f2,….fn}

Step 2: Set the policy (p1, p2, p3,…pn)

Step 3: Request to cloud server

Step 4: update{f1(p1,p2,pn), f2(p1,p2,pn), fn(p1,p2,pn),}

Step 5: Get policy update response

Step 6: display the file access policy

The above Access Policy Update steps client can dynamically changes the access right to particular upload document .For change the access right user has to send query process to cloud server. So that server will dynamically update access rights.

IV. IMPLEMENTATION AND RESULTS

The proposed HSDS-DP approach is implemented using C#.net, which is a most GUI interface and effective programming tool for research and real-time applications. The proposed system has successfully implemented as a client cloud server approach. The clients can upload file in cloud environment based on secret sharing approach, so that client can be view their upload file with High Secure manner. The data secrecy contains the several steps with less interaction with the client. This facility provides an effective result in both performance and application wise. This chapter gives the proposed system implementation steps, and the results obtained from the implementations are discussed.

IV.1.1. Implementation steps:

1. Key request to key managers
2. Get public and symmetric key
3. Breaks up symmetric key S into n shares (S1, S2, …, Sn).
4. Data Encryption and Encrypts i-th share with public key of i-th KM
5. Upload all data and shares of S to cloud
6. Download share and make a request to Key managers.
7. Receives back decrypted i-th share.
8. Reconstruct and secret share verification

V. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed schemes, security, scalability execution time and storage are the main measurement of performance evaluation. The performance of this proposed work Scheme was compared with the existing approach NTRU. Our result analysis will be focused on encryption and decryption time taken for different data size. This result shows our proposed system encryption and decryption time different is less as compared to existing system .This time different analysis details shows in graphical manner. The figure 2.0 below shows the results encryption and decryption time comparison of the proposed system

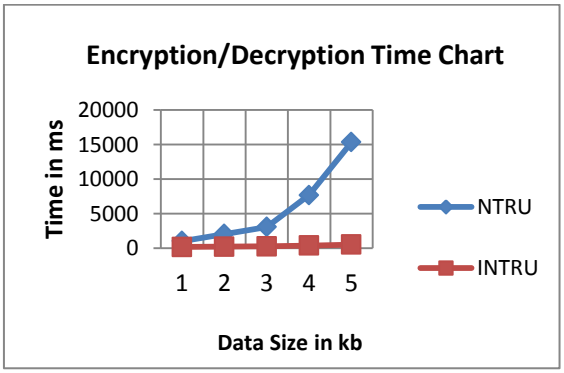


Figure 2.0 Performance of Encryption/Decryption Time chart based on accuracy

VI. CONCLUSION

Data security is more important in distributed storage system In this Project, the problem of data security in cloud data storage has been considered, To ensure the correctness and security of client s data in cloud data storage, this paper proposed an effective and flexible distributed scheme that is named as HSDS-DP (High Secure Data Share with dynamic policy update), which is a new technique for data privacy with improved security features. The proposed system implements Improved NTRU to protect the outsourced data stored in a cloud. Our scheme successfully allows the client to dynamically update the data access policy in cloud server environment.

Proposed HSDS-DP scheme that provided key management, dynamic access control, encryption process scheme achieves the integration of secure data storage. Through detailed security and performance analysis, proposed system show that our scheme is highly efficient and resilient to security failure, data attack in cloud environment. The security of our proposed scheme is guaranteed by those of the Imported NTRU cryptosystem and
the threshold secret sharing.

REFERENCES

[1].Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." Information sciences 305 (2015): 357-383.

[2]. Chandankere, Rekha, and Masrath Begum. "Secure data sharing in an untrusted cloud." Int. J. Eng. Res. Appl 5 (2015): 49-54.

[3]. Chugh, Sonam, and Sateesh Kumar Peddoju. "Access control based data security in cloud computing." International Journal of Engineering Research and Applications (IJERA) 2.3 (2016): 2589-2593.

[4]. Chou, Te-Shun. "Security threats on cloud computing vulnerabilities." International Journal of Computer Science & Information Technology 5.3 (2015): 79.

[5]. H. Takabi, J. B. D. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments" IEEE Security and Privacy, Vol. 8, No. 6, 2014,pp. 24-31.

[6] . K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dac: Effective data access control for multi authority cloud storage systems," Information Forensics and Security, IEEE Transactions on, vol. 8, no. 11, pp. 1790–1801, 2013.

[7] . Yang, Kan, Xiaohua Jia, and Kui Ren. "Secure and verifiable policy update outsourcing for big data access control in the cloud." IEEE Transactions on Parallel and Distributed Systems 26.12 (2015): 3461-3470.

[8] . Chen, Yanli, Lingling Song, and Geng Yang. "Attribute-based access control for multi-authority systems with constant size ciphertext in cloud computing." China Commun 13.2 (2016): 146-162.

Authors Profile

Mrs.P.Jayasree pursed Bachelor of Mathematices from Bharathiyar University, Coimbatore in 2005 and Master of Computer Applications from Bharathiyar University,Coimbatore in 2008 and Mater of Philosopy in Computer Science from Vinayaka Mission University, Selam in 2009 and currently working as a Assistant Professor in Department of Computer Applications**,** Hindusthan College of Arts and Science, Coimbatore, Since 2008. She has published more than 7 research papers in reputed International journals and Conferences. Her main research work focuses on Networking, DataMining, Image Processing. She has 10years of teaching experience and 5 yrs of Research experience.

V. Saravanan pursed Bachelor of Science from Madurai Kamarajar University, Madurai in 1994 and Master of Computer Applications from Bharathidasan University, Trichy in 1999 and Mater of Philosopy in Computer Science from Manonmanium Sundaranar University , Tirunelveli in 2002 and Doctorate in Computer Science from Manonmanium Sundaranar University , Tirunelveli in 2016 and currently working as Professor and Head of the Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, Since 2004. He has published more than 35 research papers in reputed International journals and Conferences. His main research work focuses on Networking, DataMining, Image Processing, Cloud Computing, Big Data Analytics, . He has 19 years of teaching experience and 15 yrs of Research experience.

