Privacy-Preserving Cipher Text Multi-Sharing Control For Big Data Storage

Bharath Kumar A L
Student, M.Tech, Network & Internet,
Dept. of ECE
Sri Jayachamarajendra college of Engineering
Mysuru, Karnataka, INDIA.

Dr. M. N. Jayara
BE,ME(IISC,Blore),PhD,LMISTE
Associate Professor, Dept. of ECE
Sri Jayachamarajendra college of Engineering
Mysuru, Karnataka, INDIA.

***Abstract*-The need of secure big data storage service is more desirable than ever to date. The Basic requirement of the service is to guarantee the confidentiality of the data. However, the anonymity of the service clients, one of the most essential aspects of privacy, should be considered simultaneously. Moreover, the service also should provide practical and fine grained encrypted data sharing such that a data owner is allowed to share a cipher text of data among others under some specified conditions. However, privacy preserving cipher text multi-sharing mechanism to achieve the above properties. It combines the merits of proxy encryption with anonymous technique in which a cipher text can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of cipher text senders/recipients. Furthermore, the paper shows that the new primitive is secure against chosen-cipher text attacks in the standard model.**

Key words: Cipher text, Multi-sharing

I. INTRODUCTION

The increase in number of individual users and public and private organizations choose to upload their data in cloud force us to keep the data more securable from being hacked. The data of an individual user should be kept confidential and it should be accessed only by the authenticated users. While providing security, the most important aspect to be considered before storing the data is that, the anonymity of the service providers. The services which are used for data storage should provide a high quality encrypted data sharing. These services provides the way that, only the cipher text of the data is shared to the authorized individuals by the data owners under some restricted and specified conditions. The features mentioned above are commonly required to maintain secure processing, and these features are achieved by employing a new technique called cipher text multi sharing mechanism. In this mechanism a proxy re-encryption technique are employed in which only the cipher text to be shared securely and conditionally over multiple times. It also ensures that, original message and information identity of cipher text senders and receivers is not leaked and it also ensures it is not vulnerable to cipher text attacks.

However,many individuals and companies choose to upload their data to clouds since the clouds supports considerable data storage service but also efficient data processing capability. Accordingly, it is unavoidable that trillions of personal and industrial data are flooding the Internet. For example, in some smart grid scenario, a governmental surveillance authority may choose to supervise the electricity consumption of a local living district. A great amount of electricity consumed data of each family located inside the district will be automatically transferred to the authority via Internet period by period. The need of big data storage, therefore, is more desirable than ever. A basic security requirement of big data storage is to guarantee the confidentiality of the data.

Security is the most important concern for any type of services which provides storage for data. Due to its efficient data processing capability cloud play a vital role in keeping big data. Many individuals and organizations can view, modify and update their data stored in the cloud through remote accessing. During remote accessing there is an possibility for some common issues like privacy, security, data integrity, dynamic updates etc… every time it is not possible to check the data for consistency, as trillions of individual and organizations data are flooding over the internet.

The specialist could begin the written work study even as the information from the unstructured and sorted out gatherings is being collected. Evaluating the written work on the point range at this time helps the researchers to think further gatherings more authoritatively on particular viewpoints found to be crucial is the appropriated studies paying little heed to the way that these had not surfaced in the midst of the before tending to. So the written work diagram is key for social event the discretionary data for the investigation which may be shown especially steady in the examination.

The proxy re-encryption systemallows the proxy to transform ciphertexts encrypted under Alice's public key into the different ciphertexts that can be decrypted by Bob's secret key. New proxy re-encryption systems; one for the transformation from ciphertexts encrypted under a traditional certificate-based public key into the ciphertexts that can be decrypted by an secret key for Identity-Based Encryption, and the other one for the transformation from ciphertexts encrypted in IBE manner into the different ciphertexts that can be decrypted by the other secret key for

the IBE. A proxy re-encryption system allows the proxy to transform ciphertexts computed under Alice's public key into the different ciphertexts that can be decrypted by using Bob's secret key. This system works as follows; Alice or a trusted third party generates a re-encryption key and sets it in a proxy. On receiving Alice's ciphertexts, the proxy transforms the ciphertext by running the re-encryption algorithm with the re-encryption key, and sends the transformed ciphertext to Bob. Bob decrypts it by his secret key. As it can be seen that Alice delegates her decryption rights to Bob via proxy, we call Alice a delegator and Bob a delegate.[1]

The proxy re-encryption system should at least satisfy the following requirements:

1) A proxy alone cannot obtain the underlying plaintext,

2) Bob cannot obtain the underlying plaintext without the proxy cooperating.

Type-based Proxy Re-encryption and its Constructionanalyze the concept of proxy re-encryption has been shown very useful in a number of applications, especially in enforcing access control policies. In existing proxy re-encryption schemes, the delegate can decrypt all ciphertexts for the delegator after re-encryption by the proxy. Consequently, in order to implement fine-grained access control policies, the delegator needs to either use multiple key pairs or trust the proxy to behave honestly. This extend the concept and proposes the type-based proxy re-encryption, which enables the delegator to selectively delegate his decryption right to the delegate while only needs one key pair. As a result, type-based proxy re-encryption enables the delegator to implement fine-grained policies with one key pair without any additional trust on the proxy. This provide a security model for our concept and provide formal dentitions for semantic security and ciphertext privacy which is a valuable attribute in privacy-sensitive contexts. Here two type-based proxy re-encryption schemes: one is CPA secure with ciphertext privacy while the other is CCA secure without cipher text privacy.[2]

Cipher Text-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE)extends the traditional Proxy Re Encryption (PRE) by allowing a semi-trusted proxy to transform a ciphertext under an access policy to the one with the same plaintext under another access policy (i.e. attribute-based re-encryption). The proxy, however, learns nothing about the underlying plaintext. CP-ABPRE has many real world applications, such as fine-grained access control in cloud storage systems and medical records sharing among different hospitals. Previous CP-ABPRE schemes leave how to be secure against chosen-ciphertext attacks (CCA) as an open problem. Here a new concept CP-ABPRE to tackle the problem. The new scheme supports attribute-based re-encryption with any monotonic access structures. Despite our scheme is constructed in the random oracle model, it can be proved CCA secure under the decisional q-parallel bilinear Diffie-Hellman exponent assumption.[3]

The Proxy re-encryption (PRE) allows a proxy to convert a ciphertext encrypted under one key into an encryption of the same message under another key. The main idea is to place as little trust and reveal as little information to the proxy as necessary to allow it to perform its translations. At the very least, the proxy should not be able to learn the keys of the participants or the content of the messages it re-encrypts. However, in all prior PRE schemes, it is easy for the proxy to determine between which participants a re-encryption key can transform ciphertexts. This can be a problem in practice. For example, in a secure distributed file system, content owners may want to use the proxy to help re-encrypt sensitive information without revealing to the proxy the identity of the recipients. In this work, key-private (or anonymous) re-encryption keys as an additional useful property of PRE schemes. This formulate a definition of what it means for a PRE scheme to be secure and key-private. Surprisingly, this show that this property is not captured by prior definitions or achieved by prior schemes, including even the secure obfuscation of PRE by Hohenberger et al. (TCC 2007). Finally, we propose the first key private PRE construction and prove its CPA-security under a simple extension of Decisional Bilinear Diffie Hellman assumption and its key-privacy under the Decision Linear assumption in the standard model.[4]

In 1998, Blaze, Bleumer, and Strauss proposed a cryptographic primitive called proxy re-encryption, in which a proxy transforms - without seeing the corresponding plaintext - a ciphertext computed under Alice's public key into one that can be opened using Bob's secret key. Recently, an appropriate definition of chosen-ciphertext security and a construction fitting this model were put forth by Canetti and Hohenberger. Their system is bidirectional: the information released to divert ciphertexts from Alice to Bob can also be used to translate ciphertexts in the opposite direction.[5]

II. IMPLEMENTATION

The usage choices are basically concerned without any difficulty of future upgrade of the framework and an appropriated situation. The necessities for execution are takes after:

1. The dialect decided for this venture is Java-Jdk-1.6
2. Windows 7 Working framework used to execute this undertake.

MySql

MySql is a social database administration framework, which arranges information as tables.

Components of Mysql

1. Customer/server structural engineering.
2. Information freedom.
3. Guaranteeing information trustworthiness.
4. Alternate preparing backing information passage and online exchange handling utilized for applications.

Modular Implementation

The project mainly has been divided in to three modules. They are:

1. User
2. Cloud Server
3. Proxy-Server

User

Description and Priority

The system will first check the user check Registered are not if user is not registered first user need to register and login to the server and then server will give permission to upload or download files.

Stimulus/Response Sequences

1. User request for registration approval from cloud server, the cloud server generate both the public and private key and forward to the appropriate user.
2. Using the registered user id and password user login to the system.
3. Next user may have rights to upload the file to the server. When user upload file the secret key and public key generated and for each file encrypt code attached as a prefix to file name.
4. User must create a group then user become a admin to the group when user become admin to the group then he upload file the user got mail of encrypted file name, secret key and public key through to user registered email id.
5. Here we generate both secret and public key for the purpose of security.
6. Then the uploaded file send to the server it is unapproved so, we cannot download the file till the server admin approved the file.

Cloud Server

Description and Priority

The Cloud Server allows user to upload or download the file after successful login using a valid username and password.

Stimulus/Response Sequences

1. The proxy server fetches the approved new users and generates a new set of keys and stores in the user account. The new keys generated by the Advanced Encryption Standard (AES) Algorithm.
2. The server received the user uploaded file and the server admin can approved the file based on some conditions like file size, check whether it may affect from any space etc.
3. This server approved files only download by the users.

Proxy-Server

Description and Priority

The Proxy-Server will work only when the main server will not in action.

Stimulus/Response Sequences

For the purposed of enhanced security purpose re-encryption is performed. While re-encryption the data uploaded by the user is once again encrypted, in order to enhance the security with double check.

III. SPECIFICATIONS AND REQUIREMENTS

Hardware Requirements

Processors	:Intel I3 2.1 GHZ.
RAM	:4 GB.
Storage	:100GB.
Monitor	:15”
Keyboard	:Standard 102 keys

Software (Tools &Technologies) Requirements

OS	: Windows
Platform	:JDK 1.7 & R 3.1.2
Language	:Java, JSP
Web Technologies	:HTML, Java Script
IDE/tool	:Net Beans 7.1

Server (Tools &Technologies) Requirements

OS	:	Apache, Tomcat
Processors	:	Intel I7 2.1 GHZ.
RAM	:	8 GB.
Storage	:	100GB.

IV. WORKFLOW

A flowchart indicates sequences and decision points as well as starting and stopping points. On resetting the power, the procedural flow starts with initialization of modules involved.

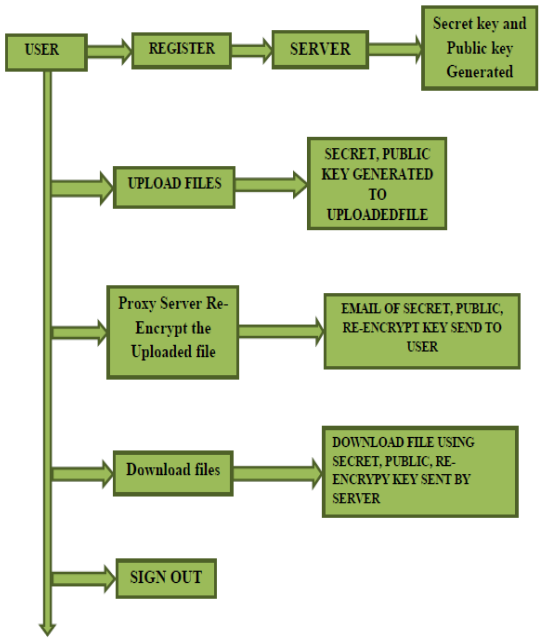

Figure 1: Flowchart

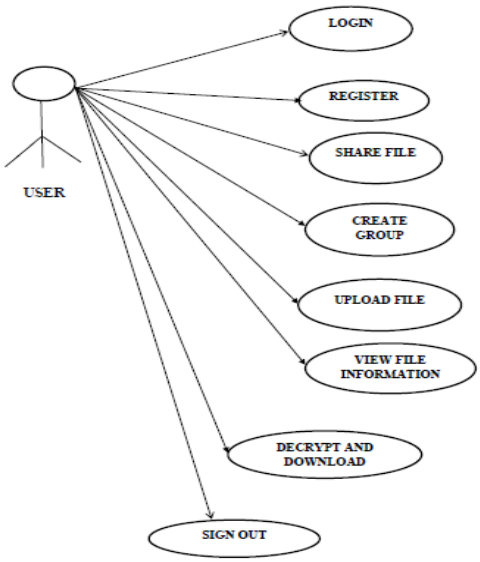

Figure 2:Case diagram for user

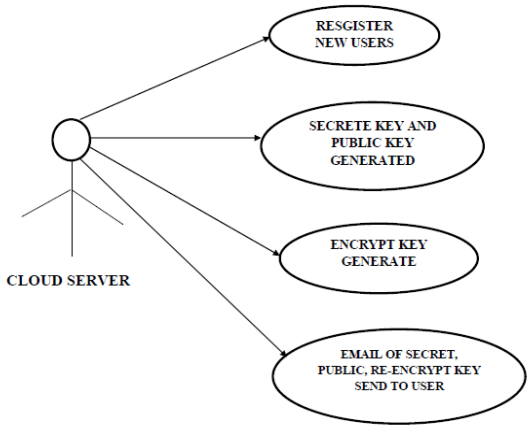

Figure 3:Case diagram for cloud server

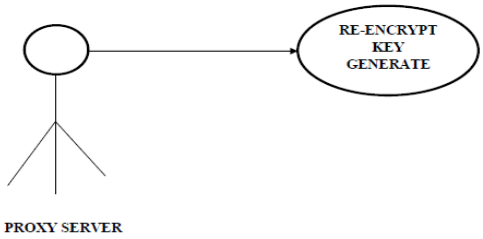

Figure 4:Case diagram for proxy server

V. CONCLUSION AND FUTURE WORK

A. Conclusion

This proposal has introduced a new mechanism known as Anonymity Multi Hop – Identity Based Conditional Proxy Re-Encryption for secure data sharing in cloud computing. This work specially focused on anonymity of the recipient and multiple cipher text of recipient which is required for protecting some sensitive confidential information while transferring the information. This mechanism also ensures consistency and efficiency of data sharing in a time consuming way and in a cheaper way. It is the first time this new mechanism is approached to ensure security against chosen cipher text attack primitives.

B. Future Work

The new mechanism proposed a concept called AMH-IBCPRE has a problem that, it provides security against some of the chosen cipher text attacks because of its unidirectional property. This unidirectional IBCPRE scheme in which a hacker is not able to identify the source properties from the encrypted destination cipher text. To safeguard the information of both sender and the receiver, a new scheme called, Anonymous-PRE (ANOPRE) was developed. This scheme guarantees that the hacker cannot identify the sender of original and re-encrypted cipher text even the re-encryption is provided. This scheme also ensures security from most of the chosen cipher text attacks. Even there are lots of models proposed for providing security, this is the only scheme that achieves all the properties, even it combine some important features of standard models.

REFERENCES

[1] C.K.Chu and W, .G.Tzeng (August 2006), “Identity-based proxy re-encryption”, (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, vol. 4779, pp. 189–202, 2006

[2] J. Shao, “Type-based proxy re-encryption,” in Information Security and Privacy (Lecture Notes in Computer Science), vol. 7372. Berlin, Germany: Springer-Verlag, pp. 364–375. 2012

[3] T. Matsuo, "Proxy re-encryption systems for identity-based encryption" in Pairing-Based Cryptography, Berlin, Germany:Springer-Verlag, vol. 4575, pp. 247-267, 2007.

[4] K. Liang, C.-K. Chu, X. Tan, D. S. Wong, C. Tang, J. Zhou, "Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts", Theoretical Comput. Sci., vol. 539, pp. 87-105, Jun. 2014.

[5] G. Ateniese, K. Benson, and S. Hohenberger, “Key-private proxy Re-encryption,” in Topics in Cryptology–CT-RSA (Lecture Notesin Computer Science), vol. 5473. Berlin, Germany: Springer-Verlag, pp. 279-294. 2009

[6] R. Canetti, S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption", *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, pp. 185-194, Oct. 2007

[7] Sun Microsystems, “Introduction to Cloud Computing Architecture”, Sun Microsystems Inc., white paper, pp. 1-17. 2009

[8] MELL, P. and GRANCE, T, “Definition of Cloud Computing”, Draft NIST working, vol.5, pp. 7-19. 2009.

[9] G. Ateniese, K. Benson, and S. Hohenberger, ,“Key-private proxy Re-encryption,” in Topics in Cryptology–CT-RSA (Lecture Notesin Computer Science), vol. 5473. Berlin, Germany: Springer-Verlag, pp. 279-294. 2009

[10] Magoulas, Roger; Lorica, Ben “Introduction to big data”, vol. Release 2.0 (Sebastopol CA: O'Reilly Media), pp.1-7. 2009,

[11] Bellare, Mihir; Rogaway, Phillip “Introduction to Modern Cryptography, by random grids, vol.1, pp.10-21. 2005,

[12] D.Boneh and X.Boyen, “Introduction”. “ID secures identity-based encryption”, Berlin, Germany: Springer-Verlag, vol.3027, pp. 223–238. 2007.