International Journal of Science and Engineering Applications
Volume 5 Issue 2, 2016, ISSN-2319-7560 (Online)

A Review on Key-Aggregate Cryptosystem for Climbable Knowledge Sharing in Cloud Storage

Priyanka Kale
Department of Computer Science And Engineering
BIT, Ballarpur, India

Mrunali Vaidya
Department of Computer Science And Engineering
BIT, Ballarpur, India

Abstract: The Data sharing is an important functionality in cloud storage. In this article, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems which produce constant-size ciphertexts such that efficient delegation of decryption rights for any set of ciphertexts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of ciphertext set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In particular, our schemes give the first public-key patient controlled encryption for flexible hierarchy, which was yet to be known.

Keywords: Cloud storage, data sharing, key-aggregate cryptosystem, Identity encryption, Attribute encryption, cryptosystem.

1.INTRODUCTION

Cloud computing is widely increasing technology; data can be saved on cloud remotely and can have access to huge applications with quality services which are shared among customers. As increase in outsourcing of data the cloud computing serves does the management of data [1].Its flexible and cost optimizing characteristic motivates the end user as well as enterprises to store the data on cloud. The insider attack is one of security concern which's needs to be focused. Cloud Service provider need to make sure whether audits are held for users who have physical access to the server. As cloud service provider stores the data of different users on same server it is possible that user's private data is leaked to others. The public auditing system of data storage security in cloud computing provides a privacy-preserving auditing protocol [2].

It is necessary to make sure that the data integrity without compromising the anonymity of the data user. To ensure the integrity the user can verify metadata on their data, upload and verify metadata [3].The main concern is how to share the data securely the answer is cryptography. The question is how can the encrypted data is to be shared. The user must provide the access rights to the other user as the data is encrypted and the decryption key should be send securely. For an example Alice keeps her private data i.e. photos on dropbox and she doesn't want to share it with everyone. As the attacker may access the data so it is not possible to rely on predefine privacy preserving mechanism so she all the photos were encrypted by her on encryption key while uploading it.

2.LITERATURE SURVEY

Cloud computing is visualized as architecture for succeeding generation. It has many facilities though have a risk of attacker who can access the data or leak the users identity. While setting a cloud users and service providers authentication is necessary. The issue arises whether loud service provider or user is not compromised. The data will leak if any one of them in compromised. The cloud should be simple, preserving the privacy and also maintaining users identity [1]

The flexible use of cloud storage for user is a need as it is seams accessing data locally though that is present at remote side. It is important to inspect the data set on the cloud. So it is necessary to allow a public audit for integrity of outsourced data through third party auditor (TPA). TPA is also beneficial for cloud service provider. It checks the correctness of the outsourced data. TPA should be able to do public audit ability, storage correctness, privacy preserving, Batch auditing with minimum communication and computation overhead[2].

There are many cloud users who wants to upload there data without providing much personal details to other users. The

anonymity of the user is to be preserved so that not to reveal the identity of data owner. Provable data possession (PDP) uses similar demonst rating marks to reduce computation on server, and network traffic. PDA ensures the data present on cloud which is un-trusted is original without accessing it. Security mediator (SEM) is approach allows the user to preserve the anonymity. Users are meant to upload all their data to SEM so that the SEM is not able to understand the data although it's going to generate the verification on data. As the users are signed at SEM it should not know the identity of up loader [3].

3.WORKING

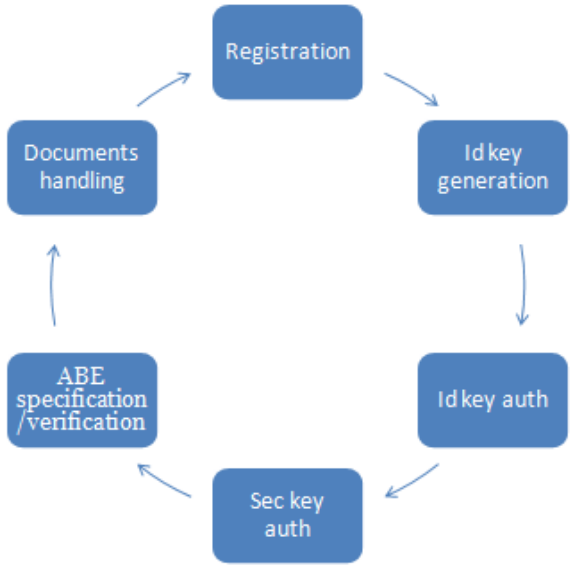

Fig .Data flow Diagram

Above figure shows how data flows between user and receiver. Firstly user registration for login with valid username and password then ID key generation and identity key authentication when the verify both key then secrete key authentication verification it goes to Attribute based encryption specification/verification of user this user valid for login or not. If user valid for login then documents handling of user, and user not valid then found error for document handling.

4 TYPEOF ENCRYPTION TECHNIQUES

4.1 Key-Aggregate Cryptosystem

New public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential.

A key-aggregate encryption system basically includes five algorithmic steps as follows- The data owner establishes the public system parameter by using Setup and generates a public/master-secret key pair by using KeyGen. Messages can be encrypted using Encrypt by anyone who also decides what ciphertext class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of ciphertext classes by Extract. The generated keys can be passed to Receivers securely via secure e-mails. Finally, any user with an aggregate key can decrypt any ciphertext provided that the ciphertext's class is contained in the aggregate key via Decrypt.

a) Setup Phase

The data owner executes the setup phase for an account onserver which is not trusted. The setup algorithm only Take simplicit security parameter.

b)KeyGen Phase

This phase is executed by data owner to generate the public or the master key pair (pk, msk).

c) Encrypt Phase

This phase is executed by anyone who wants to send the encrypted data. Encrypt (pk, m, i), the encryption algorithm takes input as public parameters pk, a message m, and I denoting cipher text class. The algorithm encrypts message m and produces a cipher text C such that only a user that has a set of attributes that satisfies the access structure is able to decrypt the message.

d) Cloud Storage

Cloud storage is nowadays very popular storage system. Cloud storage is storing of data off- site to the physical storage which is maintained by third party. Cloud storage is saving of digital data in logical pool and physical storage spans multiple servers which are manage by third party. Third party is responsible for keeping data available and accessible and physical environment should be protected and running at all time. Instead of storing data to the hard drive or any other local storage, we save data to remote storage which is accessible from anywhere and anytime. It reduces efforts of carrying physical storage to everywhere. By using cloud storage we can access information from any computer through internet which omitted limitation of accessing information from same computer where it is stored. While considering data privacy, we cannot rely on traditional technique of

authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with user's own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime to anyone. For example, organization may grant permission to access part of sensitive data to their employees. But challenging task is that how to share encrypted data. Traditional way is user can download the encrypted data from storage, decrypt that data and send it to share with others, but it loses the importance of cloud storage.

4.2 Identity encryption techniques

- System will automatically generate identity string of every user using set of different system generated algorithms
- Identity based encryption is a type of public key encryption in which public-key of a user can be set as an identity-string of the user
- At the time of registration every user will get his/her identity key on email
- While uploading and downloading documents on cloud, every user have to prove his/her identity using identity key.

4.3Attribute based encryption technique

- In this application we propose attribute based encryption technique for documents encryption
- When user wants to upload any document for particular set of users, he/she have to specify permissions in attribute format
- ABE enhances the security of system and prevent documents from leakage when attacker knows secrete key
- In order to prevent key escrow and cipher text enlargement problem we propose xml documents to store users attributes
- System will automatically create one xml doc for every user to specify his documents access attributes
- The xml document will be stored in encrypted format on server.

5. CONCLUSIONS

To share data flexibly is vital thing in cloud computing. Users prefer to upload there data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Encryption is a on solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Public-key cryptosystems provides delegation of secret keys for different cipher text classes in cloud storage. The delegate gets securely an aggregate key of constant size It is required to keep enough number of cipher texts classes as they increase fast and the cipher text classes are bounded that is the limitation.

6.ACKNOWLEDGMENTS

I would like to extend my gratitude to many people who helped me to bring this paper fruition. First I would like to thank Prof. Mrunali Vaidya. I am so deeply grateful for her help, professionalism, and valuable guidance throughout this paper. I would also like to thank to my friends and colleague. This accomplishment would not have been possible without them. Thank you.

7.REFERENCES

[1].S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE -Simple Privacy-Preserving Identity-Management for Cloud Environment,"in Applied Cryptography and Network Security –ACNS 2012, ser.LNCS, vol. 7341. Springer, 2012, pp. 526–543.

[2].C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362–375, 2013.

[3].B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Dataon the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[4].Cheng Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng,," Key Aggregate Cryptosystem for

Scalable Data Sharing in Cloud Storage ",IEEE Transaction on Parellel and Distributed System, vol. 25, no. 2, February 2014 .

[5]S.S.M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," Proc. ACM Conf. Computer and Comm. Security, pp. 152-161, 2010.

[6].S. Singh,"Different Cloud Computing Standards a Huge Challenge", The Economic times, 4 June 2009.

[7] .J. Urquhart, "The Biggest Cloud computingIssue of 2009is Trust", C-NetNews, 7 Jan 2009

[8].D. Boneh and M. K. Franklin, "Identity

-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology –CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.

[9]M. Chase and S. S. M. Chow,"Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in

CM Conference on Computer and Communications Security,
2009, pp. 121 –130.