ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data Sharing System to Avoid Inadvertent Data Leaks In the Cloud and Privacy for Preserving Data

Boga Nagesh
M.Tech (CSE)
Vignana Bharathi Institute of Technology.

N.Srinivas
Associate Professor & HOD,
Vignana Bharathi Institute of Technology.

Abstract:
Cryptography is the art and science of achieving security by encoding the message or data to make them unreadable. It is related to the aspects of network security such as privacy, reliability and accessibility of the data. A cryptosystem or cryptographic system is only the authenticated way in which user can access the encrypted data and decrypt it. The authenticated messages are shared between the authorized users. Security in cloud computing is a major concern. There are some cryptosystem techniques introduced in this security. First, Attribute Based Encryption is a public key encryption technique which is used to enable the access control over the encrypted data using qualified attributes. Second, Identity Based Encryption allows for a sender can encrypt a message to an identity without access to a public key certificate. Third, a new public key cryptosystem encrypt a message not only a public key but also under an identifier of the ciphertext classes.

Keywords: ***Cloud computing, Attribute Based Encryption, Identity Based Encryption, Key AggregateCryptosystem.***

INTRODUCTION

Cryptography is the way of storing and sharing the data in the form of that only those authenticated for it can access. It is the knowledge of securing the message by encoding it into an unreadable format. The basic goal of cryptography is the ability to send the information to the receiver in a way that prevents attackers from accessing it. This information is stored on cloud through the internet. The cloud storage is a cloud computing model in which the information is stored and remote servers are accessed from the internet. The cloud storage provider is maintaining, operating and managing the cloud storage on a server. Cryptographic mechanism is used to hide the information from unauthorized users. The most encryption algorithms can be broken and the information is stolen by the attacker. So a more realistic goal of cryptography is to make gaining the information too severe to be value it to the attacker.

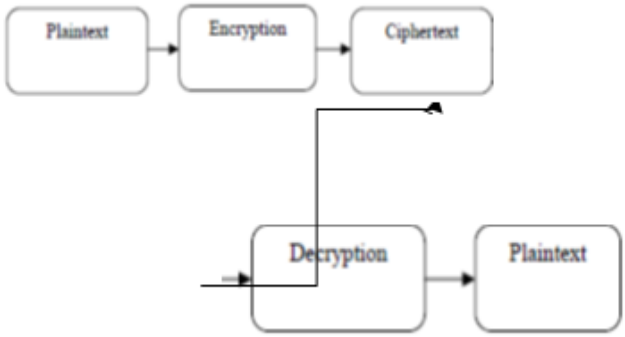


Figure 1: The encryption process converts plaintext into ciphertext and the decryption process converts ciphertexts into plaintext.

Encryption is a technique of converting original message called clear text or plaintext, into a unreadable format that can't understood by a attacker, called ciphertext. Once it can't be converted into plaintext, the user can't access it until it is decrypted. This enables the broadcast of top secret information over insecure channels without illegal disclosures. When information is stored on a computer, logical and physical access controls are confined it. When this same susceptible information is sent over a internet, it can't take longer these controls for allowed and the information is in much more susceptible state as showed in figure 1.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Encryption and decryption processes are provided by a computer system is referred to as cryptosystem and hardware components and program codes are used to create this system. The cryptosystem uses an encryption algorithm for creating a ciphertext. Most algorithms are difficult mathematical formulas that areapplied to the plaintext. Most encryption techniques use a secret value called a key, which is used to encrypt the plaintext and decrypt the ciphertext.

Figure 2: The algorithm is associated with the key and the result is applied to the message which produces the ciphertext.

In many situations, it is more important that sharing the information must be authenticated rather than encrypted. That is, both sender and receiver should be believed of each other's identity. Goal of this technique is to provide security and the access control. There are different techniques of authentication. Attribute Based Encryption was proposed by A.Sahai and B.Waters. In this scheme in which each user is identified by a set of attributes and some operations of this attributes is used to find out decryption ability for each ciphertext. Identity Based Encryption allows for a sender can encrypt a message to an identity without access to a public key certificate. This technique was proposed by Sahai and Waters. Next is the Key Aggregate Cryptosystem introduced by "Cheng-Kang Chu and Sherman S.M. Chow". This cryptosystem in which one can aggregate any set of private keys and make them as compact as a single key, but it encompass the power of all the keys being aggregated.

LITERATURE SURVEY

Authentication is used to provide privacy and security to the sensible information. Generally authentication is the way by which the computer system validates a user's gain access to information. But nowadays there are various cryptographic techniques for authentication such as Attribute Based Encryption, Identity Based Encryption, and Key aggregate cryptosystem. Goyal and Waters, "Attribute Based Encryption for Fine Grained Access Control of Encrypted Data" [2], presented a technique called Key-Policy Attribute Based Encryption (KP-ABE). In this cryptosystem, ciphertexts are labeled with set of attributes and secret keys are associated with access structures that control with ciphertexts a user is able to decrypt. While this primitive was shown to be useful for fault-tolerant encryption with biometrics, the need of expressibility seems to limit its applicability to larger system. The KP-ABE constructions do not hide the set of attributes under which information is encrypted. This is the drawback of KP-ABE cryptosystem. In 2007 Bethencourt et al. proposed a ciphertext policy attribute based encryption (CP-ABE) [3]. Data owner only believes the key provider as CP-ABE technique addresses the difficulty of KP-ABE.

Sahai and Waters, "Fuzzy Identity-Based Encryption" presented a new type of identity-based encryption that called fuzzy IBE. In fuzzy IBE, it observes an identity as set of descriptive attributes. In this technique allows for a secret key for an identity, p, to decrypt a ciphertext encrypted with an identity, q, if and only if the identities p and q are close to each other. Therefore, this scheme allows a certain amount of fault-tolerance in the identities. Fuzzy-IBE [4] produces to the two new applications. The first is an IBE system that uses biometric identities. That is it can show a user's identity such as iris scan, finger print. Since biometric measurements are noisy, we cannot use already present IBE systems. However, the fault-tolerant property of fuzzy-IBE allows for a secret key to decrypt a ciphertext encrypted with a slightly different measurement of the same biometric. Another application in fuzzy-IBE is Attribute Based Encryption. This technique is already explained in previous paragraph. The main drawback of this technique is to create a fuzzy-IBE where the attributes come from multiple authorities.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Key Aggregate Cryptosystem proposed in," Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage "by Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng , it can aggregates any set of secret key and make them as compact as single key and can be conveniently sent to other or be stored in a smart card with very limited secure storage. Andrew Chi- Chih Yao and Yunlei Zhao," Privacy-Preserving Authenticated Key-Exchange Over Internet" presents a Diffie–Hellman key exchange (DHKE), a core cryptographic mechanism for ensuring network security. For key-exchange over the Internet both security and privacy are desired. Develop a family of privacy-preserving authenticated DHKE protocols named deniable Internet key-exchange (DIKE) both in the traditional PKI setting and in the identity-based setting.

Existing System

Multi-user Searchable Encryption

Keyword search under the multi-tenancy setting is a more common scenario. In such a scenario, the data owner would like to share a document with a group of authorized users, and each user who has the access right can provide a trapdoor to perform the keyword search over the shared document, namely, the "multi-user searchable encryption" (MUSE) scenario.

Multi-Key Searchable Encryption

MKSE allows a user to provide a single keyword trapdoor to the server, but still allows the server to search for that trapdoor's keyword in documents encrypted with different keys. This might sound very similar to the goal of KASE, but these are in fact two completely different concepts.

The goal of KASE is to delegate the keyword search right to any user by distributing the aggregate key to him/her in a group data sharing system, whereas the goal of MKSE is to ensure the cloud server can perform keyword search with one trapdoor over different documents owing to a user.

Key-aggregate Encryption for Data Sharing

Data sharing systems based on cloud storage have attracted much attention recently. Consider how to reduce the number of distributed data encryption keys. To share several documents with different encryption keys with the same user, the data owner will need to distribute all such keys to him/her in a traditional approach which is usually impractical. Aiming at this challenge, a key aggregate Encryption (KAE) scheme for data sharing is proposed to generate an aggregate key for the user to decrypt all the documents.

Disadvantages

- The capability of selectively sharing encrypted data with different users via public cloud storage may greatly ease security concerns over inadvertent data leaks in the cloud.
- The implied need for secure communication, storage, and complexity clearly renders the approach impractical.

Proposed System

In this paper, address this challenge by proposing the novel concept of key-aggregate searchable encryption (KASE), and instantiating the concept through a concrete KASE scheme. The proposed KASE scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the former. To support searchable group data sharing the main requirements for efficient key management are twofold. First, a data owner only needs to distribute a single aggregate key (instead of a group of keys) to a user for sharing any number of files. Second, the user only needs to submit a single aggregate trapdoor (instead of a group of trapdoors) to the cloud for performing keyword search over any number of shared files.

Advantages

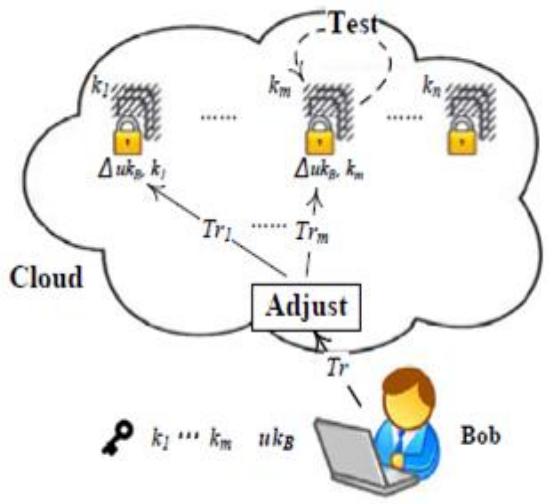
- In a KASE scheme, the owner only needs to distribute a single key to a user when sharing

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

lots of documents with the user, and the user only needs to submit a single trapdoor when he queries over all documents shared by the same owner In a practical data sharing system based on cloud storage, the user can retrieve data by any possible device and the mobile devices are widely used now.

- The security analysis and performance evaluation both confirm that our proposed schemes are provably secure and practically efficient.

System Architecture



A. AUTHENTICATION TECHNIQUES

Authentication is any process that allows one user to establish the identity of other user or entity. The old techniques of authentication are based on the originalities of the physical world; basic individualauthentication is done by identifying distinctive characteristics of other human being. In some cases, such techniques are lacking particularly when authentication must be proficient by a person who does not personally know the person to be authenticated. Some authentication methods determined to be very effective and create the base for this area of work.

1) ATTRIBUTE BASED ENCRYPTION

The ABE [2] is defined as let {A1, A2…An} be a set of parties. A collection U $\subseteq 2^{\{A1, A2....An\}}$ is monotone if ∀Q, R: if Q ∈ U and Q ⊆ R then R ∈ U. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) U of non-empty subsets of, {A1,A2,...An} i.e. U ⊆ $2^{\{A1,A2,....An\}}$.

The sets in U are called the authorized sets, and the sets not in A are called the unauthorized sets. Attribute Based Encryption scheme consists of four algorithms.

Setup: This is a randomized algorithm that takes no input other than the implicit security parameter. It outputsthe public parameters PK and a master key MK.

Encryption: This is a randomized algorithm that takes as input a message*m*, a set of attributes, and the publicparameters PK. It outputs the ciphertext *E*.

Key Generation: This is a randomized algorithm that takes as input- an access structure A, the master key MKand the public parameters PK. It outputs a decryption key

Decryption: It takes as input the user's private key SK for access structure T and the ciphertext E, which was encrypted under the attribute set. This algorithm outputs the message *m* if and only if the attribute set satisfies the user's access structure A.

The KP-ABE system would exactly allow the flexibility we predict in issuing private keys for the unique needs of each user.

2) IDENTITY BASED ENCRYPTION (IBE)

Shamir [9] first proposed the concept of Identity-Based Encryption. However, it wasn't until much later that Boneh and Franklin [3] presented the first Identity-Based Encryption scheme that was both practical and secure. Their solution made novel use of groups for which there was an efficiently computable bilinear map.To create an IBE scheme in which a ciphertext created using identity p can be decrypted only by a secret key q where |p ∩q| ≥

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

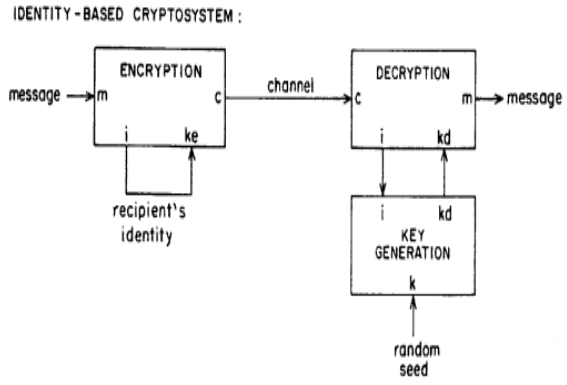


Figure 3: Identity based Cryptosystem (Identity-based cryptosystems and signature schemes [9])

Let G1 be bilinear group of prime order p, and let g be a generator of G1. Additionally, let e : G1 × G1→ G2 denote the bilinear map. A security parameter, k, will determine the size of the groups.

In this approach ciphertexts must be at least as long as the maximum number of attributes that can be required in an encryption.Adi Shamir[9] introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signature devoid of exchanging private or public keys, without keeping key directories, and without using the services of a third parties.

Chow and Waters [5] develop a new technique which allows us to circumvent this problem, and eventually build the desired IB-HPS's with almost the same complexity as the original IBEs. The idea is to add another degree of randomness to our identity-based secret keys, called the "tag" t, coupled with some master secret key terms.

A talented direction is to improve the leakage allowed from each secret key as the fraction of its size. It seems that our results can be generalized by using multiple tags in the secret key, but the security analysis is more complicated.

3) KEY AGGREGATE CRYPTOSYSTEM

In modern cryptography, a fundamental problem often studied is that leveraging the secrecy of a small piece of knowledge into the ability to perform the cryptographic functions (e.g., encryption, authentication) multiple times making a decryption key more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size. This problem is solved by introducing a special type of public-key encryption which is called as key-aggregate cryptosystem (KAC)

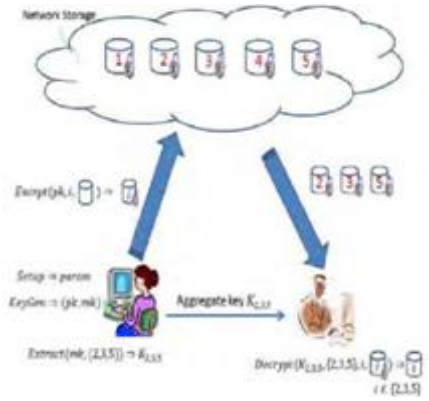


Figure 4: Using KAC for data sharing in cloud storage (Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage [1])

CONCLUSION

In this paper we have reviewed three authentication techniques: Attribute based encryption (ABE), Identity Based Encryption (IBE) and Key Aggregate Cryptosystem (KAC). The major concern in ABE is collusion-resistance but not compression of secret keys. Definitely, the ciphertext-size is not constant. In IBE, random set of identities are not match with our design of key aggregation. Key Aggregate Cryptosystem protects user's data privacy by compressing the secret key in public key cryptosystem which supports delegation of secret key for different cipher text classes. For future extension it is necessary to reserve enough cipher texts classes because in cloud cipher texts grows rapidly and the limitation is that predefined bound of the number of maximum cipher text classes.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCES

1. Baojiang Cui, Zheli Liu_ and Lingyu Wang, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS, 2015

2. 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

3. Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.

4. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

5. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology (CRYPTO '01), vol. 2139, pp. 213-229, 2001.

6. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494, pp. 457-473, 2005.

7. 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.

8. M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009,

9. C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Re-encryption without Random Oracles," Proc. Information Security Conf. (ISC '07), vol. 4779, pp. 189-202, 2007.

10. Adi Shamir, "Identity-based cryptosystems and signature schemes". In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.