International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review of Secure Data Sharing in Cloud using Key Aggregate Cryptosystem and Decoy Technology

Rushikesh V. Mahalle[1], Parnal P. Pawade[2]

[1]ME (CSE) Scholar, Department of CSE,P R Patil College of Engineering & Technology., Amravati-444604,India

[2]Assistant Professor, Department of CSE,P R Patil Engineering & Technology, Amravati-444604,India

Abstract: ***Data sharing is an important functionality in cloud storage. I show how to securely, efficiently, and flexibly share data with Decoy technology in secure cloud storage. I describe 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 force 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. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. So I provide formal security analysis of our schemes in the standard model. I 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 encryption, patient-controlled encryption

1. Introduction

The internet is a most popular one in recent years. It provides many services to users. One of the important service is cloud computing. Cloud computing is an on demand computing technology that delivers the resources as a service to the users over the internet. In cloud computing the main concern is to provide the security to end user to protect files or data from unauthorized user. Security is the main intention of any technology through which unauthorized intruder can't access your file or data in cloud. The important service provided by cloud computing is cloud storage. The local users can store their data in the remote cloud storage servers, from that the users can access the data from anywhere in the world. But storing data in a third party cloud system may affect the data confidentiality. For avoid this issue the data's are encrypted before storing in to storage server. In the general encryption system the data owner encrypts the data by using cryptographic methodology and stores the encrypted data at the cloud storage server. It provides data confidentiality but it does not provide high security and dynamic data modification. The unauthorized user may get the data while transfer from the data owner to the cloud server, or he can decrypt the data directly from the cloud server by getting cryptographic keys. Then the hacker may perform some modifications at the hacked data and again stored in to the storage server like a data owner. The cloud users and data owner can't identify the data hacking. The data displays like original data. The receiver thing like the data came from the data owner; it affects the data originality, data origin authentication, security and data integrity. Encryption keys also come with two flavors—symmetric key or asymmetric (public) key. Using symmetric encryption, when user wants the data to be originated from a third party, she has to give the encryptor her secret key; obviously, this is not always desirable. By contrast, the encryption key and decryption key are different in public key encryption. The use of public-key encryption gives more flexibility for our applications. For example, in enterprise settings, every employee can upload encrypted data on the cloud storage server without the knowledge of the company's master-secret key. Cloud computing is Internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to computers on a pay-as-you-use basis. Users can access these services available on the "internet cloud" without having any previous knowledge on managing the resources involved. Thus, users can concentrate more on the core business processes rather than spending time on gaining knowledge on resources needed to manage their business processes. Data from different clients can be hosted on separate virtual machines but reside on a single physical machine. Data in a target VM could be stolen by instantiating another VM coresident with the target one. Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owner's anonymity. These users are motivated to encrypt their data with their own keys before uploading them to the server.

2. Literature Survey

Cloud is market-oriented distributed computing systems consisting of a collection of inter- connected and virtualized computers.In cloud computing, users can outsource their computation and storage to servers using Internet. The field of cryptography deals with the techniques for conveying information securely. The goal of cryptography is to allow the intended recipients of a message to receive the message securely. Cryptography tries to prevent the eavesdroppers from understanding the message. The message in its original form is called plaintext. The transmitter of a secure system

Licensed Under Creative Commons Attribution CC BY

will encrypt the plaintext in order to hide its meaning. This meaning will be revealed only after the correct recipient tries to access it. This reversible mathematical process produces an encrypted output called cipher-text. The algorithm used to encrypt the message is a cipher. The unauthenticated user can also try to access the information. The analysis is carried out to check if cipher's security is satisfactory from unauthorized access. Cryptanalysis is the science of breaking ciphers, and cryptanalysts try to defeat the security of cryptographic systems. A cipher-text can be transmitted openly across a communications channel. Because of its encrypted nature, eavesdroppers who may have access to the cipher-text will ideally be unable to uncover the meaning of the message. Only the intended recipient, who has the valid key, can decrypt the message to recover the plaintext and interpret. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou,[1] In this paper authors explain about How to protect users' data privacy is a central question of cloud storage. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this article,I consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size.Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges. Boyang Wang, Sherman S. M. Chow, Ming Li, and Hui Li[2],This paper they introduce what they believe is the right approach to achieve anonymity in storing data to the cloud with publicly-verifiable data-integrity in mind. In their approach decouples the anonymous protection mechanism from the provable data possession mechanism via the use of security middleman. In their solution not only minimizes the computation and bandwidth requirement of this middleman, but also minimizes the trust placed on it in terms of data privacy and identity privacy. The efficiency of our system is also empirically demonstrated. Yong Cheng, Jiangchun Ren, Zhiying Wang, Songzhu Mei, Jie Zhou[3],In this paper presents a novel technique, attributes union, for promoting the CP-ABE algorithm's applications in cryptographic access control systems. Attributes unionizing means that I can reduce the number of components in ciphertext and private secret keys. And I can reduce the storage and computational overhead to a constraint by unionizing attributes. The attributes union can be also used for modifying other existing CP-ABE algorithms. We benefit a lot from attributes union, since the number of attributes only has a mini effect on it. Ashish Agarwala, R Saravanan [4],The working of the algorithm is based on the careful selection of the parameters specified. Values of p and q should be large enough to make the modulus n very large. Values of b and r should be such that br is much smaller than n. To ensure br is smaller than n, b should be much smaller than n and r should be much smaller than (n). Fengli Zhang, Qinyi Li1, Hu Xiong [5], Here, they give the efficiency analysis and comparing of some existence revocable ABE schemes. |PK|, |CT| and |SK| present the size of public parameters, the overhead of the ciphertext and the size of user's private key, respectively. Security model is denoted by "Sec-Model" which demonstrates the scheme can be proved either in full security model and selective security model. P.Jyothi1, R.Anuradha2, Dr.Y.Vijayalata,[6] In this paper they implemented a prototype application that demonstrates proof of concept of a security mechanism presented by Stolfo et al. [7]. The security mechanism focuses on preventing insider data theft attacks. This is achieved by using two technologies together. They are known as user profile management and offensive decoy technology. These two approaches together could prevent insider data theft attacks. The user profile management ensures that the legitimate users' behavior and navigational patterns are recorded. The decoy technology allows the application to keep decoy information or Fake information in the file system to deceive insider data theft attackers. When malicious insiders enter into the cloud file system, they materially get attracted to decoy information.

Table 1: Different types of Concept

Title of the Paper	Authors	Year/ISSN No./Volume Number	Proposed Concept and Details
Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage	Cheng Kang Chu, S.S.M.Chow	February 2014/Vol 25/ No. 2	A new public- key cryptosystems that produce constant-size ciphertext with private keys to decrypt
Storing Shared Data on the Cloud via Security-Middleman	B. Wang, S.S.M. Chow, M. Li, H. Li	(ICDCS)/2013	Security middleman which is able to generate verification signatures for data owners.
Attributes Union in CP-ABE Algorithm for Large Universe Cryptographic Access Control	Yong Cheng, Jiangchun Ren, Zhiying	Vol I /Nov 2012/180-186	A novel technique namedn *attributes union*, which can integrate a certain number of attributes into an attributes union
A Public Key Cryptosystem Based on Number Theory	Ashish Agarwala, R.Saravanan	April 2012 /238-241	It is based on number theory and exploits the features of computation - ally hard problems, namely integer factorization, discrete logarithmic problem to name a few.

Licensed Under Creative Commons Attribution CC BY

3. Proposed Work

In modern cryptography, the key aggregate policies is use to make a decryption of key more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size. A special type of public-key encryption which call key-aggregate cryptosystem. In KAC, users encrypt a message not only under a public-key, but also under an identifier of ciphertext called class. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for various classes. More importance, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes. The sizes of ciphertext, public-key, and master-secret key and aggregate key in our KAC schemes are all of constant size. The public system parameter has size linear in the number of ciphertext classes, but only a small part of it is needed each time and it can be fetched oxmsn demand from large cloud storage.

The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen. Messages can be encrypted via 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 via Extract. The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally, any user with an aggregate key can decrypt any ciphertext provided that the ciphertex's class is contained in the aggregate key via Decrypt.

3.1 User Behavior Profiling

By monitoring data access in the cloud and detect abnormal data access patterns User profiling is a well-known Technique that can be applied here to model how, when, and how much a user entrances their information in the Cloud. Where behavior is continuously checked to determine whether abnormal access to a user's information is occurring. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would materially include sizable information, how many documents are typically read and how often. I monitor for abnormal search behaviors that exhibit deviations from the user baseline the correlation of search behavior anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's cleanness.

3.2 Decoy Technology

Decoy technology is the technology which is providing the decoy information to the unauthorized user or the attacker. Decoy technologies for example honeypot, or the generating The useless data files on the demand of the system to do attack against the attacker. Using this technique the original information gets changed in unexpected format so that the ex-filtering of the document or information is becomes impossible.

Decoy means the relative disinformation, Fake information about the respective data documents. This technology is mainly stores some of the decoy data files in the database of the customer as the part of his database. As the decoy files are in same database of the user so that the attacker is gets failed to verify between the actual documents and decoy documents. As the attacker is going to continuing the attack on user's data documents so there is direct linking fog computing sites. So the Fake documents getting receive to the attacker in the much more amount. As the Fake data is gets downloaded by the attacker he gets confused among which data is the actual targeted data. But all the documents are of the Fake types so the original data is gets secured from the malicious insider attack.

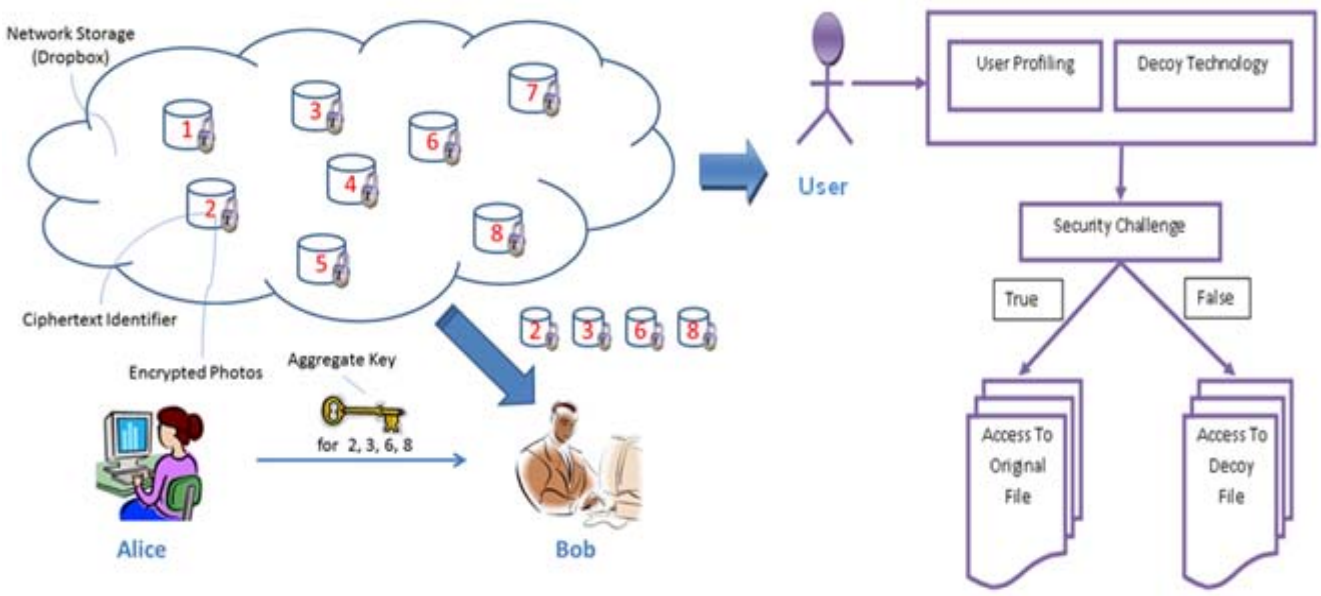


Figure 1: System Architecture

Licensed Under Creative Commons Attribution CC BY

4. Conclusions

The aggregate key encryption combined with ciphertext, which prevent attacks with high security. Key distribution can be managed easily with perfect security. The access policy and cryptographic schemes are getting more versatile and often involve multiple keys for a single application. Approach is more flexible than other key assignment which can only save a data.

References

[1] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Senior Member, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," IEEE Transaction on Parallel and Distributed System, Vol. 25, NO. 2, February 2014.
[2] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Middleman," Proc. IEEE 33rd Int‟l Conf. Distributed Computing Systems (ICDCS), 2013.
[3] Yong Cheng, Jiangchun Ren, Zhiying Wang, "Attributes Union in CP-ABE Algorithm for Large Universe Cryptographic Access Control," Second International Conference on Cloud and Green Computing,pp.180-186, Nov 2012.
[4] Ashish Agarwala, R Saravanan, "A Public Key Cryptosystem Based on Number Theory" Recent Advances in Computing and Software System (RACSS), pp. 238-241, April 2012.
[5] Fengli Zhang, Qinyi Li, Hu Xiong, "Efficient Revocable Key-Policy Attribute Based Encryption with Full Security," Eighth International Conference on Computational Intelligence and Security,pp. 477-481,Nov 2012.
[6] P.Jyothi1, R.Anuradha2, Dr.Y.Vijayalata3, "Minimizing Internal Data Theft in Cloud Through Disinformation Attacks," International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013.
[7] G.Jai Arul Jose, C.Sajeev, "Implementation of Data Security in Cloud Computing", International Journals of P2P Network Trends and Technology, Vol. 1, Issue 1, 2011.

Licensed Under Creative Commons Attribution CC BY