Data Sharing in Cloud Computing Based On Attribute Based Encryption System

K. Subha[1], P. Kushal Reddy[2], D. Sai Teja[3], O. Sunil Reddy[4], P. Satya Tarun Reddy[5]

1. Assistant Professor, Department of CSE, SRM University, Chennai.
2. U.G Scholar, Department of CSE, SRM University, Chennai.
[kushalreddy95, domakuntlasaiteja, orugantisunilreddy, satyatarun18]@gmail.com

Abstract:

A data owner (DO) is usually store large amounts of data in cloud for saving the cost on local data management. Without any data protection mechanism, cloud service provider (CSP), however, can fully gain access to all data of the user. Data owner can fully control the access policy associated with his data which to be shared. However, CP-ABE is limited to a potential security risk that is known as key escrow problem whereby the secret keys of users have to be issued by a trusted key authority. The proposed system revisits the attribute-based data sharing scheme in order to not only to solve the key escrow issue but also to improve the expressiveness of attribute, so that the resulting scheme is friendly to cloud computing applications. The proposed system has an improved two-party key issuing protocol that can guarantee that neither key authority nor cloud service provider can compromise the whole secret key of a user individually. This brings a potential security risk to the user, since CSP may compromise the data for commercial benefits. Ciphertext-policy attribute-based encryption (CP-ABE) has turned to be an important encryption technology to tackle the challenge of secure data sharing.

Index Terms: Data Protection Mechanism, Attribute-based encryption, Removing escrow, Cloud computing.

1. Introduction

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging

in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

Advocates claim that cloud computing allows companies to avoid up-front infrastructure costs (e.g., purchasing servers). As well, it enables organizations to focus on their core businesses instead of spending time and money on computer infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables Information technology (IT) teams to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This will lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

In 2009, the availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service oriented architecture, and autonomic and utility computing led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale down again as demands decrease. In 2013, it was reported that cloud computing had become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Some cloud vendors are experiencing growth rates of 50% per year, but being still in a stage of infancy, it has pitfalls that need to be addressed to make cloud computing services more reliable and user friendly.

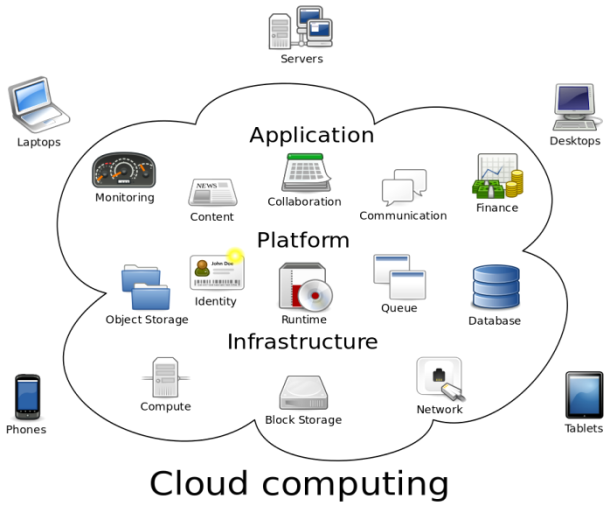

Fig. 1. Basic View of Cloud Computing

II. Related work

In 2014, Liming Fang and Willy Susilo [1] introduced Ciphertext-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 another ciphertext with the same plaintext under a new 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. All the existing CP-ABPRE schemes are leaving chosen-ciphertext attack (CCA) security as an interesting open problem. This paper, for the first time, proposes a new CP-ABPRE scheme to tackle the problem. The new scheme supports attribute-based re-encryption with any monotonic access structures. Despite being constructed in the random oracle model, our scheme can be proven CCA secure under the decisional q-parallel bilinear Diffie–Hellman exponent assumption.

[2]Smart grid is a technological innovation that improves efficiency, reliability, economics, and sustainability of electricity services. It plays a crucial role in modern energy infrastructure. The main challenges of smart grids, however, are how to manage different types of front-end intelligent devices such as power assets and smart meters efficiently; and how to process a huge amount of data received from these devices. Cloud computing, a technology that provides computational resources on demands, is a good candidate to address these challenges since it has several good properties such as energy saving, cost saving, agility, scalability and flexibility. We propose a secure cloud computing based framework for big data information management in smart grids, which we call “Smart-Frame.” The main idea of our framework is to build a hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis. In addition to this structural framework, we present a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework.

[3]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 ciphertext of data among others under some specified conditions. This paper, for the first time, proposes a privacy-preserving ciphertext multi-sharing mechanism to achieve the above properties. It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of ciphertext senders/recipients. Furthermore, this paper shows that the new primitive is secure against chosen-ciphertext attacks in the standard model.

[4] With the increasing popularity of online social networks (OSNs) and the ability to access and exchange sensitive user information, user privacy concerns become an important issue which has attracted the attention of researchers and policymakers. For example, deleted

pictures or pictures in deleted posts may not be deleted from the OSN server immediately, and hence accessible to another unauthorized user. In this paper, we highlight the deletion delay issue in seven popular OSNs, namely: Facebook, Instagram, MySpace, Tumblr, Flickr, Google+ and Weibo, which can be exploited by another unauthorized user to gain access to these pictures. To ensure OSN users are able to achieve a higher level of privacy, we propose a conceptual privacy-preserving tool for photo sharing, without compromising on transparency and real-time sharing features. We demonstrate the utility of the tool by prototyping a browser extension, which does not require modification of existing OSN systems.

[5]We define a general notion for proxy re-encryption (PRE), which we call deterministic finite automata-based functional PRE (DFA-based FPRE). Meanwhile, we propose the first and concrete DFA-based FPRE system, which adapts to our new notion. In our scheme, a message is encrypted in a ciphertext associated with an arbitrary length index string, and a decryptor is legitimate if and only if a DFA associated with his/her secret key accepts the string. Furthermore, the above encryption is allowed to be transformed to another ciphertext associated with a new string by a semi-trusted proxy to whom a re-encryption key is given. Nevertheless, the proxy cannot gain access to the underlying plaintext. This new primitive can increase the flexibility of users to delegate their decryption rights to others. We also prove it as fully chosen-ciphertext secure in the standard model.

III. System Model

As illustrated in Fig.2, the system model of CP-ABE scheme in cloud computing are given, where the system consists of four types of entities: KDC, CS, DO, and End User. In addition, we provide the detailed definition of CP-ABE scheme.

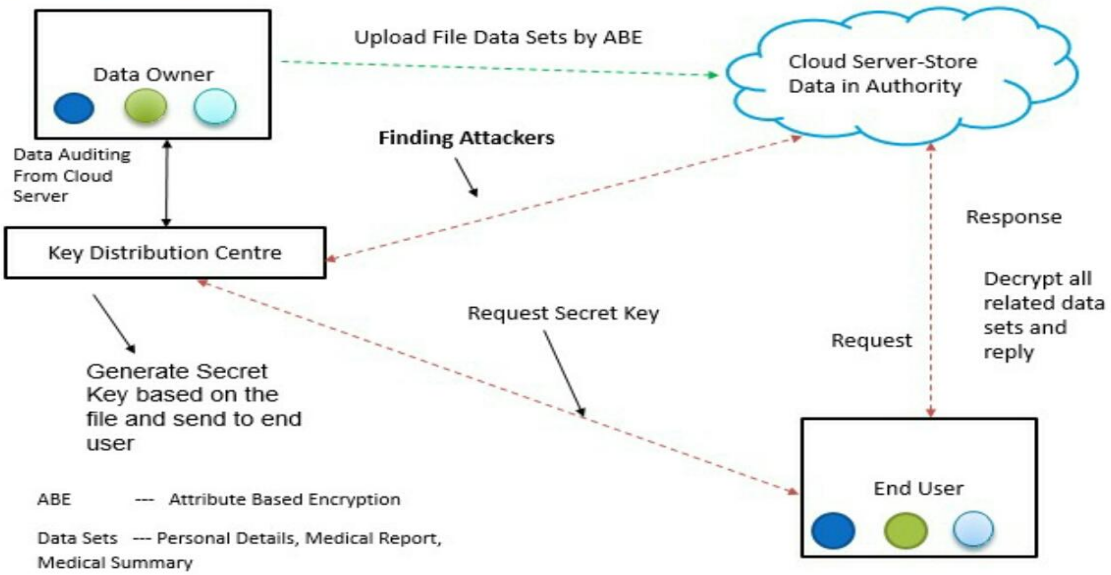

Fig.2. System model of CP-ABE scheme in Cloud Computing.

Key Distribution Center (KDC)

It is a semi-trusted entity in cloud system. Namely, KDC is honest-but-curious, which can honestly perform the assigned tasks and return correct results. However, it will collect as many sensitive contents as possible. In cloud system, the entity is responsible for the users' enrollment. Meanwhile, it not only generates most part of system parameter, but also creates most part of secret key for each user.

Cloud Server (CS)

It is also a semi-trusted entity which provides many services such as data storage, computation and transmission. To solve the key escrow problem, it generates both parts of system parameter and secret key for each user.

Data Owners (DO)

They are owners of files to be stored in cloud system. They are in charge of defining access structure and executing data encryption operation. They also upload the generated ciphertext to Cloud Server.

End User:

End users are those who want to access the ciphertext stored in cloud server. They download the ciphertext and execute the corresponding decryption operation.

IV. Modules

In this Proposed System there are 5 different modules which are:

- Key Distribution Center
- Data Owner
- Cloud server
- End User
- Attacker

Key Distribution Center

Key Distribution Center who is trusted to store verification parameters and offer public query services for these parameters such as generating secret key based on the file and send to the corresponding end users. It is responsible for capturing the attackers.

Data Owner

The data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

Cloud Server

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. It is responsible for authorizing all end users.

End User

The user can only access the data file with the encrypted key, if the user has the privilege to access the file. For the user level, all the privileges are given by the Data owner and the Data users are controlled by the data owner only. Users may try to access data files either within their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. He is sending request to Key Distribution Center to generate secret key and Key Distribution Center will generate the secret key and send to corresponding end user.

Attacker

Attacker adds the malicious data to a block in cloud server. The unauthorized user who tries to get access to the data will be considered as an attacker.

IV (a) . Implementation OF Modules

When comes to the implementation process, we are using mainly two algorithms which are:

- Cipher text-policy attribute-based encryption (CP-ABE)
- The Diffie -Hellman algorithm.

Cipher text-policy attribute-based encryption (CP-ABE)

[6],[7]cipher text-policy attribute-based encryption (CP-ABE) system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the cipher text, stating what kind of receivers will be able to decrypt the cipher text. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority. Such a user can decrypt a cipher text if his/her attributes satisfy the access policy associated with the cipher text. Thus, CP-ABE mechanism is conceptually closer to traditional role-based access control method. The first CP-ABE scheme was proposed by Bettencourt et al. in, but its security was proved in the generic group model. Cheung and Newport gave a CP-ABE construction under the Bilinear Diffie-Hellman assumption, but policies are restricted to a single AND gate. Later, Goyal Proposed a generic transformational approach to transform a KP-ABE scheme into a CP-ABE scheme using universal access tree in. Their construction can support access structures which can be represented by a bounded size access tree with threshold gates as its nodes, and its security proof is based on the standard Decisional Bilinear Diffie-Hellman assumption. Unfortunately, in general this methodology would yield a cipher text blowup of group elements for a Boolean formula of size, which limits its usefulness in practice. The most efficient CP-ABE schemes in terms of cipher text size and expressivity were proposed by Waters in, the size of a cipher text depending linearly on the number of attributes involved in the specific policy for that cipher text.

The Diffie-Hellman algorithm

[8]This algorithm uses arithmetic modulus as the basis of its calculation. Suppose Alice and Bob follow this key exchange procedure with Eve acting as a man in middle interceptor (or the bad guy). Here are the calculation steps followed in this algorithm that make sure that eve never gets to know the final keys through which actual encryption of data takes place.

First, both Alice and Bob agree upon a prime number and another number that has no factor in common. Let's call the prime number as **p** and the other number as **g**. Note that **g** is also known as the generator and **p** is known as prime modulus.

- Now, since eve is sitting in between and listening to this communication so eve also gets to know **p** and **g**.
- Now, the modulus arithmetic says that **r** = (**g** to the power **x**) mod **p.** So **r** will always produce an integer between 0 and **p**.
- The first trick here is that given **x** (with **g** and **p** known), it's very easy to find **r**. But given **r** (with **g** and **p** known) it's difficult to deduce **x**.
- One may argue that this is not that difficult to crack but what if the value of **p** is a very huge prime number? Well, if this is the case then deducing **x** (if **r** is given) becomes almost next to impossible as it would take thousands of years to crack this even with supercomputers.
- This is also called the discrete logarithmic problem.
- Coming back to the communication, all the three Bob, Alice and eve now know **g** and **p**.
- Now, Alice selects a random private number **xa** and calculates (**g** to the power **xa**) mod **p** =**ra**. This resultant **ra** is sent on the communication channel to Bob. Intercepting in between, eve also comes to know **ra**.
- Similarly Bob selects his own random private number **xb**, calculates (**g** to the power **xb**) mod **p** = **rb** and sends this **rb** to Alice through the same communication channel. Obviously eve also comes to know about **rb**.
- So eve now has information about **g**, **p**, **ra** and **rb**.
- Now comes the heart of this algorithm. Alice calculates (**rb** to the power **xa**) mod **p** = **Final key** which is equivalent to **(g to the power (xa*xb)) mod p**.

V. Performance Analysis

Now, to validate theoretical analysis proposed in previous subsection, we execute CP-WABE-RE scheme by using the CP-ABE toolkit and the Java Pairing-Based Cryptography library (JPBC). Meanwhile, we also simulate the schemes in [9],[10] and at the same condition. The following experiments are conducted using Java on the system with Intel(R) Core(TM) i5-4590 CPU at 3.30 GHz and 8.00GB RAM running Windows 7. To achieve 80-bit security level, the experiments use a 160-bit elliptic curve group based on the super singular curve $y^2 = x^3 + x$ over a 512-bit finite field. In addition, all the simulation results are the mean of 10 trials. The units of storage cost and time are Kilobyte (KB) and second (s).

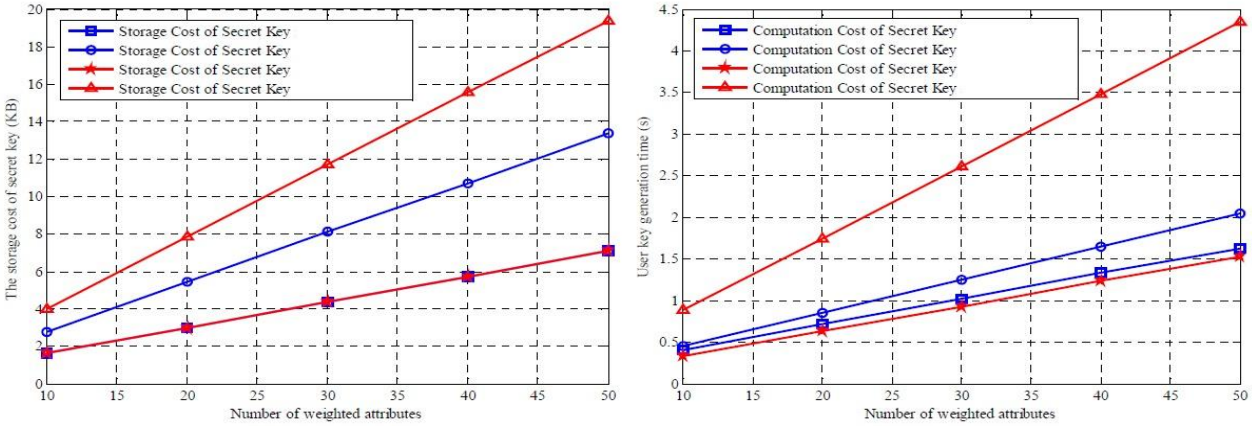

Fig. 3. Comparison of experimental results of key escrow. (a)The storage cost of secret key. (b)The time cost of user key generation

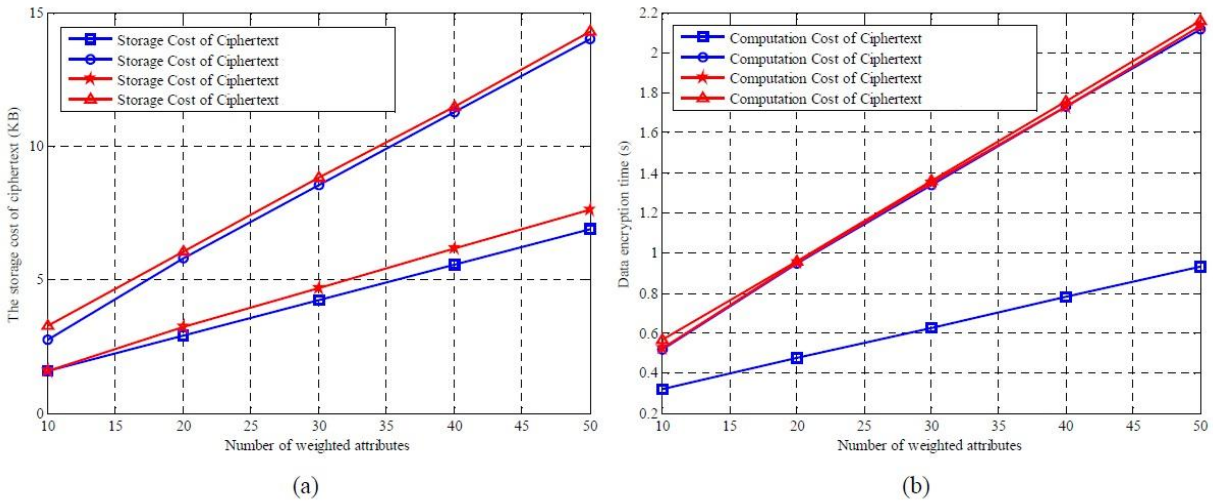

Fig. 4. Comparison of experimental results of weighted attribute. (a) The storage of ciphertext. (b) The time cost of encryption.

VI. Conclusion And Future Work

In this paper, we redesigned an attribute-based data sharing scheme in cloud computing. The improved key issuing protocol was presented to resolve the key escrow problem. It enhances data confidentiality and privacy in cloud system against the managers of KA and CSP as well as malicious system outsiders, where KA and CSP are semi-trusted. In addition, the weighted attribute was proposed to improve the expression of attribute, which can not only describe arbitrary state attributes, but also reduce the complexity of access policy, so that the storage cost of ciphertext and time cost in encryption can be saved. Finally, we presented the performance and security analysis for the proposed scheme, in which the results demonstrate high efficiency and security of our scheme. Our future work includes an upgrade model which can not only find

attackers but also the attackers can be removed from the on- going transaction which enhances more secure data sharing.

REFERENCES

[1] Kaitai Liang, Willy Susilo. A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds. Concurrency and computation. (Volume 2, Issue 8, 10 June 2015 Pages 2004-2027.
[2] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A secure cloud computing based framework for big data information management of smart grid. *IEEE Transactions on Cloud Computing*, 3(2):233–244, 2015.
[3] Joseph K. Liu , Willy Susilo, Kaitai Liang. Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage. IEEE Transactions on Information Forensics and Security (Volume: 10, Issue: 8, Aug. 2015)
[4] Shangqi Lai, Joseph K. Liu, Kim-Kwang Raymond Choo. Information and communications security.
[5] Man HO Au, Duncan S Wong, Guomin Yong. A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing. IEEE Transactions on Information Forensics and Security (Volume: 9, Issue: 10, Oct. 2014).
[6] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu, and W. Shi. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. *Information Sciences*, 275(11):370–384, 2014.
[7] C. Fan, S. Huang, and H. Rung. Arbitrary-state attribute-based encryption with dynamic membership. *IEEE Transactions on Computers*, 63(8):1951–1961, 2014.
[8] Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98, 2006.
[9] J. Hur. Improving security and efficiency in attribute-based data sharing. *IEEE Transactions on Knowledge and Data Engineering*, 25(10):2271 – 2282, 2013.
[10] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker. Mediated ciphertext-policy attribute-based encryption and its application. *Proceedings of the 10th International Workshop on Information Security Applications*, pages 309–323, 2009