A Secure Outsourced Encryption Based Access Control Model for Cloud Based Services

Karem Swathi[1], M Chandrasekhar varma[2]
[1]M.Tech Scholar, Dept. of Computer Science Engineering,
[2]Assis Professor. Dept. of Computer Science Engineering, DNR College of Engineering &Technology, Bhimavaram, AP, INDIA.
Corresponding Author: Karem Swathi

ABSTRACT: With the rapid development of computer technology, cloud-based services have become a hot topic. They not only provide users with convenience, but also bring many security issues, such as data sharing and privacy issue. In this paper, we present an access control system with privilege separation based on privacy protection (PS-ACS). In the PS-ACS scheme, we divide users into private domain (PRD) and public domain (PUD) logically. In PRD, to achieve read access permission and write access permission, we adopt the Key-Aggregate Encryption (KAE) and the Improved Attribute-based Signature (IABS) respectively. In PUD, we construct a new multi-authority ciphertext policy attribute- based encryption (CP-ABE) scheme with efficient decryption to avoid the issues of single point of failure and complicated key distribution, and design an efficient attribute revocation method for it. The analysis and simulation result show that our scheme is feasible and superior to protect users' privacy in cloud-based services.

Keywords: Privacy control Access, Cloud Computing, Security framework

Date of Submission: 29-11-2018 Date of acceptance: 13-12-2018

I. INTRODUCTION

With the rapid development of cloud computing, big data and public cloud services have been widely used. Users can store their data in the cloud service and rely on the cloud service provider to give data access to other users. However, the cloud service provider can no longer be fully trusted. Because it may give data access to some illegal users or attackers for profit gain. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. Therefore, the study of access control scheme to protect users' privacy in cloud environment is of great significance. Since traditional access control strategy [1] cannot effectively solve the security problems that exist in data sharing, various schemes to achieve encryption and decryption of data sharing have been proposed. In 2007, Bethencourt et al. [2] first proposed the ciphertext policy attribute-based encryption (CP-ABE). However, this scheme does not consider the revocation of access permissions. Attrapadung et al. [3, 4] came up with two user-revocable ABE scheme. However, they are not applicable in the outsourcing environment. In 2011, Hur et al. [5] put forward a fine grained revocation scheme, but it can easily cause key escrow issue. Lewko et al. [6] used multi-authority ABE (MA-ABE) to solve key escrow issue. But the access policy is not flexible. Later, Li et al. [7] presented a data sharing scheme based on systemic attribute encryption, which endows different access permissions to different users. However, it lacks of efficiency. Xie et al. [8] presented a revocable CPABE scheme. Compared with Hur's scheme, in the key update phase, the computation load of the data service manager will be reduced by half. Liang et al. [9] proposed a CP-ABE proxy encryption scheme which supports any monotonic access structures. However, their construction which is built in the composite order bilinear group cannot be converted to the prime order bilinear group. In 2014, Chu et al. [10] proposed Key-Aggregate Encryption algorithm, which effectively shortens the length of the ciphertext and the key, but only for the situation where the data owner knows user's identity. The above schemes only focus on one aspect of the research, and do not have a strict uniform standard either. In this paper, we present a more systematic, flexible and efficient access control scheme. To this end, we make the following main contributions:

1) We propose a novel access control system called PS-ACS, which is privilege separation based on privacy protection. To achieve read access permission, in PRD, the Key-Aggregate Encryption (KAE) scheme which greatly improves access efficiency is adopted. And in PUD, we construct a new multi-authority ciphertext policy attribute-based encryption (CP-ABE) scheme with efficient decryption to avoid the issues of single point of failure and complicated key distribution, and design an efficient attribute revocation method for it.

2) Compared with the MAH-ABE scheme which does not refer to the write access control, we exploit an Improved Attribute-based Signature (IABS) [11-13] scheme to enforce write access control in PRD. In this

way, the user can pass the cloud server's signature verification without disclosing the identity, and successfully modify the file.

3) We provide security and performance analysis of our proposed PS-ACS scheme. The functionality and simulation results provide data security in acceptable performance impact, and prove the feasibility of the scheme.

II. PRIVACY PROTECTION METHODS

Various methods have been put forward to overcome this issue of privacy preserving. This work studies some of those approaches and provides a concise outline. It is important, that the privacy has to be preserved anytime and anywhere. The protection can be done by both provider and user at server side and client side.

2.1 Encryption Strategies

The data can be encrypted and decrypted before storing in the cloud. User can encrypt their data while uploading it on the cloud and decrypt while downloading it. In [3], review of various encryption schemes is provided.

2.1.1 Key Policy Attribute Based Encryption

A set of descriptive attributes is labeled by the encrypt or for each cipher text. An access structure is associated with Each private key that indicate which form of cipher-texts the key can decrypt. In the work of Jin sun [4], the key policy ABE is associated with the broadcast encryption to provide a dual system encryption. With this standard model, the scheme can achieve fixed-size public criterion, force no bound on attribute set size used for encryption.

2.1.2Cipher-text policy Attribute Based Encryption

Here attribute policies are associated with data and attributes are associated with keys. Decryption is possible only those keys which are collaborated with attributes satisfy the policy collaborated with the data. This encryption satisfies the security needs demanded by the customer.

2.1.3Cipher-text policy Attribute Set Based Encryption

A recursive set-based structure is framed by organizing user attributes and allows users to demand dynamic constraints on how those attributes may be associated to satisfy a policy. By using this techniques encrypted data can be kept secret even if the storage server is not trustworthy; moreover, this method provide security against collusion attack. This methods are related to conventional access control methods such as Role-Based Access Control (RBAC).

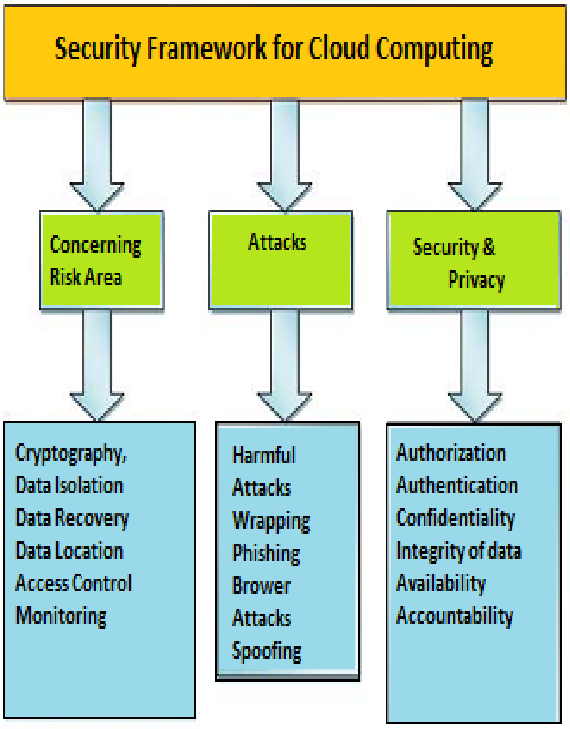
Security Framework for Cloud Computing
Concerning Risk Area
Attacks
Security & Privacy
Cryptography, Data Isolation Data Recovery Data Location Access Control Monitoring
Harmful Attacks Wrapping Phishing Brower Attacks Spoofing
Authorization Authentication Confidentiality Integrity of data Availability Accountability

Fig 1: A framework for secure cloud computing.

2.1.4 Fuzzy Identity-Based Encryption

As measured by the overlap distance metric, the identities a and a’ should be close to each other then only it is possible to decrypt a cipher-text encrypted with an identity a’ with a private key for an identity a. In fuzzy, a biometric can also be used as attributes for the identities.

2.2 Identity Based Authentication

In [5], SSL Authentication Protocol is applied in cloud computing, will become so complicated that users will undergo a bulk point both in computation and communication. It based on the identity-based hierarchical model for cloud computing. In [6], the authors proposed a dynamic authentication protocol that can support dynamic operations in cloud. This enables only valid users to authenticate in cloud.

III. DESIGN IMPLEMENTATION

Data Owner:

Proposed Key-Aggregate Encryption algorithm, effectively shortening the length of the ciphertext and the key, but only for the situation where the data owner knows the user's identity. Personal domain (PSD), in which users have special privileges, such as family, personal assistant, close friends and partners. This domain has a small number of users and small scale attributes, and the data owner knows the user's identity, which is easy to manage. Data Owner, based on the characteristics of users in public and personal domain to develop different access control strategy, encrypt uploaded files using the corresponding encryption method and then send to the cloud server. The data owner only wants the users to access or modify parts of data files, and different users can access and modify different parts of the data. For example, the blogger can allow his friend to browse part of his private photos; enterprises can also authorize employees to access or modify part of sensitive data.

User:

Cloud based services not only provide users with convenience, but also bring many security issues. Therefore, the study of access control scheme to protect users' privacy in cloud environment is of great significance. We divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, we set read and write access permissions for users respectively. The Key-Aggregate Encryption (KAE) is exploited to implement the read access permission which improves the access efficiency. The users of PUD, a hierarchical attribute-based encryption (HABE) is applied to avoid the issues of single point of failure and complicated key distribution. Function and performance testing result shows that the PS-ACS scheme can achieve privacy protection in cloud based services. The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy.

Cloud:

For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. Therefore, we need to develop an effective access control solution. Data security issues brought by data sharing have seriously hindered the development of cloud computing, various solutions to achieve encryption and decryption of data sharing have been proposed. The user can pass the cloud server’s signature verification without disclosing the identity, and successfully modify the file.

IV. ACCESS CONTROL SCHEME IN PRD

The PRD has a small number of users, and their identities are known to the owner. In general, the data owner only wants the users to access or modify parts of data fi les, and different users can access and modify different parts of the data. For example, the blogger can allow his friend to browse part of his private photos; enterprises can also authorize employees to access or modify part of sensitive data. This requires the data owner to grant users read or write access permission to some data. In Chen’s [15] MAH-ABE scheme, the CP-ABE is used to achieve the read access permission, but there are some defects to be considered. Firstly, since in PRD, each user has a close relationship with the owner and the number is small, there is no need to use the CP-ABE which is applicable to the scenario which has a lot of users, and their identities are unknown to the owner, while the KAE scheme is set for the small users with certain identities. Besides, the distribution and management of keys and attributes, encryption and decryption process of CP-ABE are much more complex compared with the KAE scheme. Therefore, the KAE scheme is adopted to achieve the read access permission which improves the access efficiency.

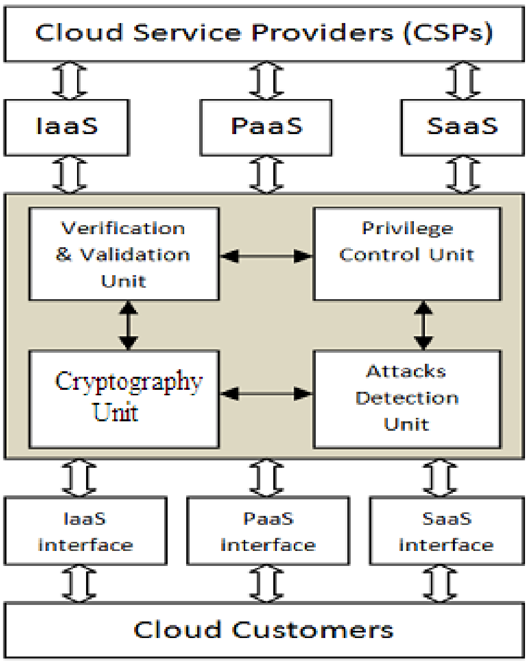

Fig 2. Cloud Computing Security Model

Schematic Rules for Robust Key Aggregate Cryptosystems
1. Setup (1λ,n) : The Information owner establishes a parameter for public systems via Setup. On input of a security level parameter 1λ and number of cipher text classes n, it outputs the public system parameter param
2. KeyGen: It is executed by information owner to randomly generate a public/M Secret key (Pk,msk) 3. Encrypt (Pk,i,m): It is executed by data owner and for message m and index i, it computes the ciphertext as C
4. Extract (msk,S): It is executed by information owner for attending the decrypting power for a particular set of cipher text classes and it outputs the aggregate key for set S denoted by Ks
5. Decrypt (Ks,S,I,C): It is executed by a delegate who received, an random key Ks, created by extract. On input Ks, set S, an index I denoting the ciphertext class ciphertext to and output is decrypted result m.

V. ACCESS CONTROL SCHEME IN PUD

The PUD is characterized by a huge number of users, a lot of attributes owned by the user, complexity management, and indefinite users' identity. In view of the above characteristics, the user can only have the read access permission. Although the attribute-based encryption scheme (CP-ABE) can achieve access control, it cannot meet the needs of complex cloud environment. In traditional CP-ABE scheme, there is only one attribute authority responsible for the management of attributes and distribution of keys. The authority may be a university registrar's office, the company's HR department or government educational organizations and so on. The data owner defines access policies and encrypts the data files in accordance with this policy. Each user is distributed a key related to his attribute. As long as the user's attributes meet the access policy he can decrypt the file.

However, if there is only one authority in the system and all public and private keys are issued by the authority. Two problems will appear in the practical application:

1) In the practical cloud environment, there are a lot of authorities and each authority in their own field manages part of users' attributes. The attributes owned by the user are issued from different authorities. For example, a data owner may want to share his medical data with a user who owns the doctor attribute issued by medical institutions and the medical researcher attribute by the clinic practice man secret Othagement. Therefore, exploiting multi authority is more realistic in the practical scenarios.

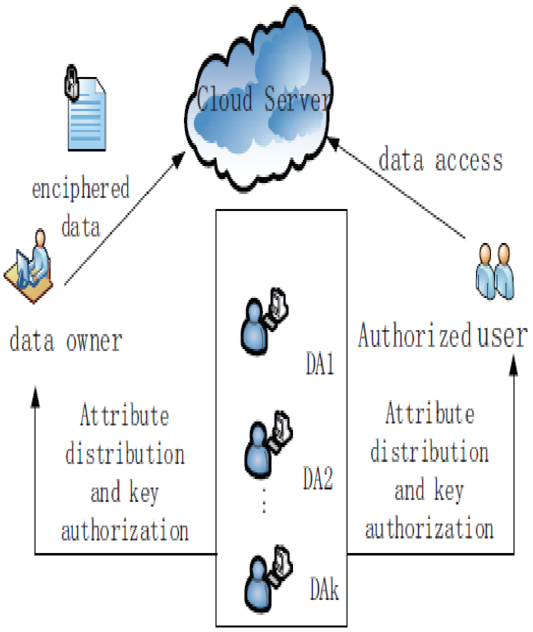
Cloud Server
enciphered data
data access
data owner
Authorized user
DA1
DA2
DAk
Attribute distribution and key authorization
Attribute distribution and key authorization

Fig 3. Access control framework of PUD

Therefore, multi authority ABE (MA-ABE) is used in this paper. To reduce the computation overhead of users in PUD, we propose an outsourcing decryption MA-ABE scheme. Firstly the data owner uploads the attribute-based encrypted data files to the cloud server. When a user requests the encrypted data from the cloud server, the cloud server will first check his transformation key. Only if the corresponding attributes satisfy the access structure, will the cloud server output a partially decrypted ciphertext and then sends it to the user. Finally, upon receiving the partially decrypted ciphertext, the user can use his private key to recover the message. The framework of this area is shown in Fig.3

VI. CONCLUSION

In this paper, we proposed an access control system (PS-ACS), which is privilege separation based on privacy protection. Through the analysis of cloud environment and the characteristics of the user, we divide users into personal domain (PRD) and public domain (PUD) logically. In PRD, we set read and write access permissions for users respectively. To achieve read access permission, the KAE scheme which can improve the access efficiency is adopted. A high degree of patient privacy is guaranteed simultaneously by using IABS scheme which can determine users' write access permission. For users in PUD, we constructed a new multi-authority ciphertext policy attribute-based encryption (CP-ABE) scheme with efficient decryption to avoid the issues of single point of failure and complicated key distribution, and design an efficient attribute revocation method for it. The analysis and the simulation result show that the PSACS scheme is feasible and superior to protect the privacy of data in cloud-based services.

REFERENCES

[1]. S. Yu, C. Wang, K. Ren, "Achieving secure, scalable, and fine-grained data access control in cloud computing," Proc. IEEE INFOCOM, pp. 1-9, 2010.

[2]. J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption," Proc. Security and Privacy, pp. 321-334, 2007.

[3]. J. Hur, D.K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions.

[4]. A. Lewko, B. Waters, "Decentralizing attribute-Based encryption," Proc. Advances in Cryptology-EUROCRYPT, pp. 568-588, 2011.

[5]. M. Li, S. Yu, Y. Zheng, "Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encryption," IEEE Transactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131- 143, 2013.

[6]. C.K. Chu, S.S.M. Chow, W.G. Tzeng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, 2014.

[7]. J. Li, K. Kim, “Hidden attribute-based signatures without anonymity revocation,” Information Sciences, vol. 180, no. 9, pp. 1681-1689, 2010.

[8]. H.K. Maji, M. Prabhakaran, M. Rosulek, “Attribute-Based Signatures,” Proc. Topics in Cryptology - CT-RSA, pp. 376-392, 2011.

[9]. S. Kumar, S. Agrawal, S. Balaraman, “Attribute based signatures for bounded multi-level threshold circuits,” Proc. Public Key Infrastructures, Services and Applications, pp. 141-154,2011.

Karem Swathi. " A Secure Outsourced Encryption Based Access Control Model for Cloud Based Services. "IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 12, 2018, pp. 71-76.