Volume No:4, Issue No:2 (July-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Confidential Security based Access Control Scheme in CBS (Cloud-based Services)

Shaik Nageena
Department of Computer Science & Engineering,
MJR College of Engineering & Technology, Piler, AP- 517214, India.

Mr. Kotari Suresh
Department of Computer Science & Engineering,
MJR College of Engineering & Technology, Piler, AP- 517214, India.

Karamala Suresh
Department of Computer Science & Engineering,
MJR College of Engineering & Technology, Piler, AP- 517214, India.

ABSTRACT:
With the quick advancement of PC innovation, cloud-based administrations have turned into a hotly debated issue. They furnish clients with comfort, as well as bring numerous security issues, for example, information sharing and protection issue. In this paper, we show an entrance control framework with benefit detachment in view of security insurance (PS-ACS). In the PS-ACS plot, we isolate clients into a private area (PRD) and open space (PUD) legitimately. In PRD, to accomplish read get to authorization and compose get to consent, we embrace the Key-Aggregate Encryption (KAE) and the Improved Attribute-based Signature (IBS) separately. In PUD, we build another multi-specialist ciphertext approach quality based encryption (CP-ABE) conspire with productive decoding to stay away from the issues of single purpose of disappointment and entangled key conveyance, and plan a proficient property repudiation strategy for it. The investigation and reproduction result demonstrates that our plan is practical and better than ensure clients' security in cloud-based administrations.

Keywords: Access control; data sharing;

I. INTRODUCTION:

With the fast development of cloud computing, big data and public cloud services have been extensively used. The user can store their data in the cloud. Although cloud computing brings great advantage to business and customers, the cloud computing security has always been a major risk.

For customers, it is necessary to take full advantage of cloud storage service, and also to provide data privacy. Therefore, we need to promote an effective access control solution. Since the traditional access control strategy [1] cannot effectively solve the security problems that occur data sharing. 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. In 2007, Bethencourt et al. [2] first proposed the cipher text policy attribute-based encryption (CP-ABE). However, this scheme does not consider the revocation of access permissions. In 2011, Hur et al. [3] put forward a fine-grained revocation scheme but it can easily cause key escrow issue. Lewko et al. [4] used multi authority ABE (MA-ABE) to solve key security issue. But the access policy is not flexible. Li et al [5] presented data sharing scheme based on fundamental attribute encryption, which enhance different users' different access rights. But it is not efficient from the complexity and efficiency. In 2014, Chen et al. [6] proposed Key-Aggregate Encryption algorithm, effectively shortening the length of the cipher text and the key, but only for the situation where the data owner knows the customer's identity. These schemes only focus on one aspect of the research, and do not have a strict uniform standard

Cite this article as: Shaik Nageena, Mr. Kotari Suresh & Karamala Suresh, "Confidential security based Access Control Scheme in CBS (Cloud-based Services)", International Journal of Research in Advanced Computer Science Engineering, Volume 4, Issue 2, 2018, Page 5-9.

Volume No:4, Issue No:2 (July-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

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 new access control system called PSACS, which is advantage separation based on privacy protection. The system uses Key-Aggregate Encryption (KAE) scheme and Hierarchy Attribute-based Encryption (HABE) scheme to develop read access control scheme in the PSD and PUD commonly. The KAE scheme greatly improves access efficiency and the HABE scheme largely reduces the task of a single authority and supports the privacy of user data.

2. Compared with the MAH-ABE scheme which does not refer to the write access control, we accomplishment an Improved Attribute-based Signature (IABS) [7-9] scheme to require write access control in the PSD. In this way, the customer can pass the cloud server's signature verification without disclosing the identity, and successfully updating the file.

3. We furnish a complete analysis of security and complexity of our proposed PS-ACS scheme. The functionality and simulation results produce data security in acceptable performance impact, and prove the feasibility of the scheme.

II. EXISTING SYSTEM:

As shown in Fig.1, system model consists of Data holders, Customers in PSD, and users in PUD, root authority CA, regional authority AA and cloud service vendor, which are defined as follows.

1. The cloud service vendor consists of two parts: information storage server and information service management. Information storage server is answerable for storing high security data files, and information service management is in charge of controlling the users' access to secret data and returning the corresponding cipher text.

2. In the certain cloud environment, CA manages multiple AA, and AA each manages attributes in their own area. The attributes owned by the customer are issued by different authority.

3. Personal domain (PSD), in which customers have exclusively privileges, such as family, personal assistant, close friends and partners. This domain has a small number of customers and small scale attributes, and the information owner knows the customer's identity, which is easy to maintain.

4. Public domain (PUD), which owns a large number of users with unknown identity and a lot of attributes owned by the customer.

5. Information 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 sends to the cloud server.

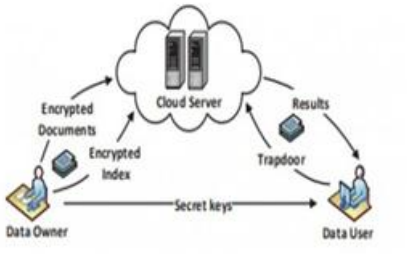

Fig:1. System framework

III PROPOSED SYSTEM:

This may cause a tremendous overhead on the expert particularly in huge scale cloud frameworks, where membership trapdoors might be every now and again created/ refreshed. Therefore, one test is the manner by which to "coordinate" membership arrangement registering with quality based access control of the distributed information, rather than utilizing another arrangement of ABE parameters.

ACCESS CONTROL SCHEME IN PSD

A. Read Access Control

The PSD has a small number of customers, and their identities are known to the holder. In general, the data holder only wants the customers to access or change parts of data files, and different customers can access and change different parts of the information.

Volume No:4, Issue No:2 (July-2018)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

For example, the blogger can allow their friend to browse part of his private photos; enterprises can also authorize employees to access or modify part of sensitive data. This needs the data holder to grant customers read or write access permission to some information. In Chen's MAH-ABE scheme, the CP-ABE is used to obtain the read access permission, but there are some errors to be considered. Firstly, since in the PSD, the customers are all have a close relationship with the holder and the number is small, there is no need to use the CP-ABE which is useful to the scenario which has a lot of customers, and their identities are unknown to the holder, while the KAE scheme is set for the small customers 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 is exploited to develop the read access permission which upgrades the access efficiency.

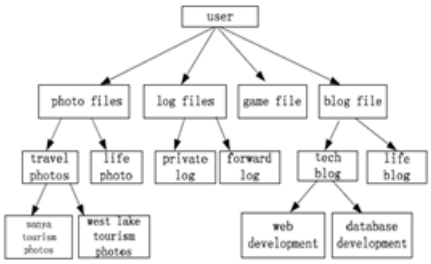

Fig: 2. Data file classification

B. Write Access Control:

As Chen's MAH-ABE scheme does not invoke to the write access control and in the PSD some cases exist, for example, the holder requires their friends to modify their file after he/she read it. So we proposed the write access permission in the PSD. For the user, the public key and file class label are all known; he/she can implement the algorithm to encrypt the files after he/she updated, and then upload them to the cloud. But whether the cloud server saves the updated file is decided by the write access control policy. On the one hand, in the cloud environment, if a customer's modification operations are very recurrent, maybe he is very essential to the customer, so that the customer may be harmed from outside attacks. Therefore, the user worries the leak of identity after the signature. On the other hand, in the data sharing scheme, the separate access of read and write to the file is extremely essential. In PSD, not all users who have read permissions also have write permissions to the files. Whether the user has write permissions to the data file is decided by the data holder. Therefore, this paper selects the improved attribute-based signature (IABS) to determine the customer's write permission. The main structure of the scheme includes five parts: an authentication center (CA), the data holder, customers, mediator and cloud servers. The CA is responsible for generating master key which is sent to the owner and system parameters which are shared for all customers. The mediator holds part components of the signature keys and is responsible for the validity check of attributes and users. The data owner produces the signature tree and sends it directly to the cloud server. The user encrypts the updated files and signs them using the attribute-based signature, then uploads them to the cloud server. The cloud server verifies the attribute-based signature, if the authentication is successful; the user has permission to update files and the cloud server stores the file. Own to the limited space we will eliminate the specific description of the IABS scheme in PSD.

ACCESS CONTROL SCHEME IN PUD

A. Scheme Design:

The PUD is characterized by a large number of customers, a lot of attributes owned by the customer, complexity management, and indefinite customer identity. The customer 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 single authorized agency responsible for the management of attributes and distribution of keys.

Volume No:4, Issue No:2 (July-2018) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The authority may be a university office, the company's HR department or government educational institutions and so on. The data holder defines access policies and encrypts the data files in accordance with this policy. Every customer 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 single authority in the system and all public and private keys are issued by the authority. Two major problems will occur 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 customer's attributes. The attributes owned by the customer are issued from different authorities. For example, a data holder may want to share his medical information with a customer who owns the doctor attribute issued by medical institutions and the medical researcher attribute by the clinic practice management. Therefore, exploiting multi authority is more realistic in the practical scenarios.
2. If there is only single authority, all the distribution of the keys is handed over by one trusted authority. The continue interaction between the customer and trust authority will not only bring bottlenecks for the system load capacity, but also enhance the potential security risks. Therefore, multi authority ABE (MA-ABE) is used in this paper. Customers in PUD do not need to interact directly with the data holder, and the attributes of the user are called role attributes. Firstly the data holder uploads the attribute-based encrypted information files to the cloud server.

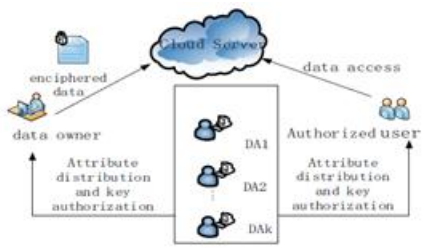

Fig 3. Access control framework of PUD

The framework of this area is shown in Fig.3. Then after authorized, the data holder receives the corresponding decryption key and sends a information file access request directly from the cloud server. Finally, after the cloud server returns the cipher text, customer can use their own decryption key to decrypt the cipher text.

B. Access Control Process:

Based on the above analysis, we use a hierarchical attribute encryption scheme (HABE) to develop access control in PUD.

1. Files creation: The creating of files is completed by the data holder. In general, in order to protect the privacy of the information file, the data holder firstly encrypts data file, and then stores it in the cloud.

2. Data access: If the user wishes to access a data file, he/she should get the file from the cloud server and decrypt the encrypted information file, which corresponds to the decryption process.

Files deletion: If the data holder wishes to delete a file, he/she can send the file ID and his signature SG to the cloud server, then the cloud servers remove the files after checking the signature of the data holder.

IV CONCLUSION:

In this paper, we propose access control system (PS-ACS), which is privilege separation based on privacy protection. Through the analysis of cloud environment and the characteristics of the customer, we divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, the KAE algorithm is applied to develop customer read access permissions and greatly improved efficiency. The IABS scheme is employed to achieve the write permissions and the separation of read and write permissions to protect the privacy of the customer's identity. In the PUD, we use the HABE scheme to stop the issues of single point of failure and to achieve data sharing. By comparing with the MAH-ABE scheme, the proposed scheme shows the feasibility and superiority to protect the privacy of data in cloud-based services.

Volume No:4, Issue No:2 (July-2018)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

V 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 on Parallel and Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2011.

[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.

Author's Profile:

Shaik Nageena

Pursuing M.Tech at MJR College of Engineering & Technology, Department of CSE, Piler, Chittoor Dist.

Kotari Suresh

Working as a Assistant Professor in MJR College of engineering & technology, Department Of CSE, Piler, Andhra Pradesh.

Karamala Suresh

Working as a Head of the Department in MJR College Of Engineering And Technology, Department Of Cse, Piler, Chittoor dist. He is having 14 years of teaching experience in engineering colleges, he received B.Tech(CSE) from JNTU Hyderabad in 2002,Received M.E(CSE) from satyabama university Chennai in 2006,and Received M.Tech(CSE) in 2015 from JNTU Anantapuramu, he published several research papers in various national and international journals. He is interested in Computer Networks.