ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 11(48), DOI: 10.17485/ijst/2018/v11i48/138791, December 2018* ISSN (Online) : 0974-5645

Secure Access Control Scheme for Data Sharing Using KAE and Attribute Authority Based CP-ABE Schemes

D.S.C. Reddy and Papisetty Saranya*

Department of CSE, PBR Visvodaya Institute of Technology and Science, Nellore - 524201, Andhra Pradesh, India; saranyacse039@gmail.com, srujand@hotmail.com

Abstract

Objective: To study the access control scheme to protect users' privacy problem in cloud environment is great significance. To overcome the above problem we build a new access control scheme with privilege separation based on privacy protection. **Methods/Statistical Analysis:** Data sharing is one of the key features which change the business/individuals life style in store and share data using clouds. But it also poses data privacy issues. To this effect, in this study we develop a scheme named as PS-ACS (Privacy protection based Access control scheme), which uses cloud servers to store and share the owners' data; for that cloud server divides the users into private and public platforms. And also analyzes the Key Aggregate Encryption (KAE) and Improved Attribute-Based Signature (IABS) to manage the read and write access rights of users in private platform. Also re-evaluates the Hierarchical Attribute-based Encryption which is applied to avoid the bottleneck issue in public platform. **Findings:** Here, we consider the data files of user's private photos, blog data, log files, and business files which required data owners to grant the access rights to read or modify the private data. To protect the data privacy, we use KAE and IABS to build the PS-ACS while sharing the data to the cloud users. In this study, we also show our scheme is protects the data privacy rather than existing techniques. **Applications/Improvements:** We have used different encryption schemes in two different platforms which protect the data privacy efficiently and also we extend our scheme to avoid the single point of failure using HABE efficiently.

Keywords: Access Control, Attribute Based Signature Scheme, Data Sharing, Privacy Protection, User Revocation

1. Introduction

For users, it is necessary to take full advantage of cloud-based storage service, and conjointly to warrant information privacy. Therefore, we have to ensure a far better access management mechanism[1]. Since, the previous access management techniques cannot provide complete safety to information sharing efficiently. Information security risks brought by data sharing can critically mired in the implementation of cloud computing, many solutions to attain encode and decode of knowledge sharing are projected.

Many authors planned varied techniques to safeguard the privacy of users. In[2] presented the Cipher text-policy Attribute-Based Encryption (CP-ABE), but which does not assume the revocation of access rights. In[3] presented the most straightforward revocation plan anyway it coordinates to key update issue. In[4] specified Multi-Authority ABE (MA-ABE) to solve key update issue. However, the access rights are not applicable. In[5] introduced information sharing system supported general attributes based cryptography, which offers various access rights to the various users. However, it is inefficient for the complexities.

In[6] presented Key-Aggregate Encryption in which it is difficult to encode the elements of the cipher text and the corresponding key, though exclusively inside the conditions once the information proprietor receptive to the client's attributes. These plans over the sole point on one component of the investigation, and can't offer a

*Author for correspondence

strict uniform typical either. Amid this study, we will, in general, enrich an extra adaptable, orderly and efficient access the executive's topic. To the current end, we will, in general, achieve the ensuing principle commitments:

- We initiate a novel access rule structure called PS-ACS, which is permission set separated based on security protection. The framework uses Key-Aggregate Encryption (KAE) plan and Hierarchy Attribute-based Encryption (HABE) plan to convey read access to control plot in the PSD and PUD separately. The KAE plan broadly made access ability and the HABE plot basically reduce the job of a particular authority and defends the security of customers' data.
- Evaluated with the MAH-ABE system which cannot bother to the write permission management, we develop an Improved Attribute-Based Signature (IABS)[7,8] plan to perform write permission in the Personal Domain (PSD).
- We benefit a wise investigation of security and hinders of our proposed PS-ACS strategy. The results guarantee information privacy and show the practicability of the proposed plan.

2. Research Method

2.1 System Framework

As illustrated in Figure 1, our system comprises Data owner, users in PSD, and users in PUD, root authority CA, regional authority AA and cloud service provider, and are defined as follows:

- The cloud provider comprises two sections: an information storage server and information service Management. The data storage server is in risk of securing private data files, and information service management is responsible for compelling unapproved customers access to grouped data and gives the relating cipher text.
- In the real cloud environment, CA handles numerous AA, and every AA manages attributes of their own field. The attributes which are claimed by the client were offered by a different AA's.
- Personal domain (PSD) where clients have unique privileges, for example, family, individual colleague, dear companions and accomplices. This domain has

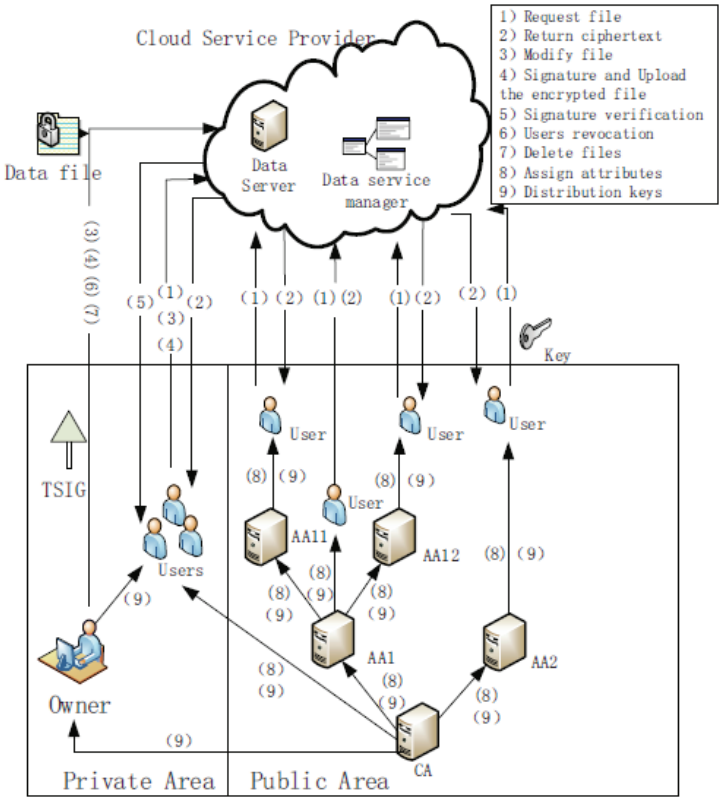

Figure 1. System Framework.

a couple of clients and little scale attributes, and the owner has the client's identity, which is simple to manage.
- Public domain (PUD), which involves a few clients with an uncertain personal identity and every client, claims a lot of attributes.
- Data Owner, based on the attributes of customer's public and personal domain to distinctive access control approach encode transferred records utilizing the ensuing encryption technique and afterward advances to the cloud server.

2.2 Access Control Scheme in PSD

2.2.1 Read Access Control

The PSD has minor number of clients in which the owner distinguishes every client identity. Nonetheless, the owner needs the clients to get encoded parts of information records, and various clients can get and modify the parts of the information.

There is a need that an owner offers customers to read or write privilege for data. In Chen's MAH-ABE plan, the CP-ABE is used to accomplish the read access, yet there were a couple of troubles to be considered. Initially, since in the Domain, the customers are all have a close relation with the owner and the number is small, so it is no convincing motivation to use the CP-ABE which has a different number of customers, and relating identities are new to the owner, while the procedure for KAE is set for the little customers with definite identities.

Besides that the allotment and the management of keys and attributes, encryption and decryption system of CP-ABE are astoundingly multifaceted rather than KAE strategy. However, the KAE is oppressed to the read privilege which enhance the read accessibility effectively. The KAE process is shown in following steps:

- System setup and file encryption: The system executes Setup of KAE to create general system parameter and a master key. Each owner classifies the record by its information attributes, like "photo files", "blog files" and "game files". Figure 2 shows the classification of various files.
- Access and key distribution: In this when the consumer sends the access request to the server of the cloud, and his file index is i, then the server sends back the resulting encoded document to the consumer.
- The owner authorized customers access privilege with the document index indicated by j and also the gathering S of all the indicator j sent to CA, CA can get the decoding key of customers for a group of cipher text through concentrate of KAE, Ultimately, any customer with the aggregate key can decipher any cipher text with an aggregate key.

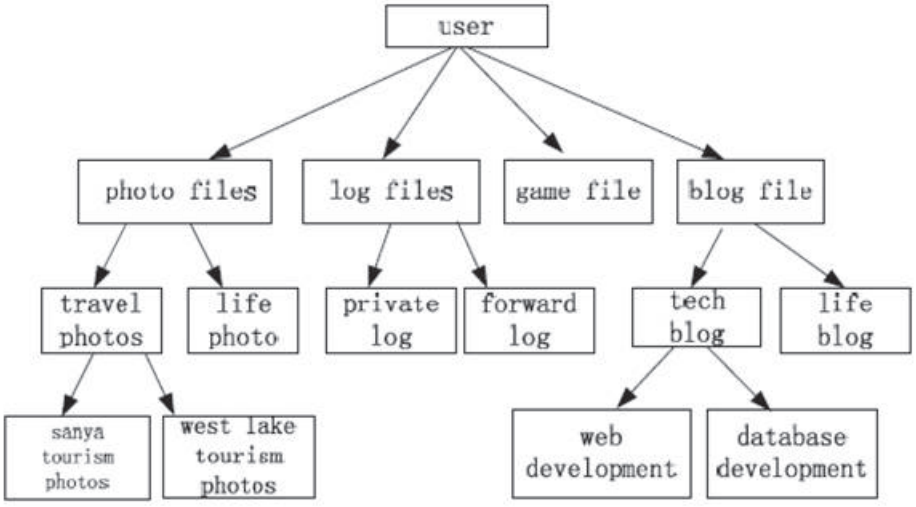

Figure 2. Data Files Classification.

2.3 Write Access Control

In the PSD, the write access permission of customers is before allowing the users to alter the documents. So we implemented write access privileges in the PSD. For the customers, the public key and document class mark are altogether known to the client, the user can understand the work process of a plan to perform encryption of records after the user modified, and then transferred to the cloud. But, whether the cloud server stores the altered document is examined by the write access strategy.

In this entire procedure, the signature leak is kept clients in dilemma. Likewise, in the information sharing plan, the access rights are assuming the crucial task. In this area, every client who has read permission is not having write permission. The owner of the information must think about the client who has to write access thus we implement Improved Attribute-Based Signature plan in this study.

The structure of the scheme includes five segments: an authentication center (CA), the Data Owner, customers, mediator and cloud servers. The CA who is in-charge of generating a master key which is sent for owner and system parameters which are shared by the customers. The mediator grips part components of the sign keys and is responsible for testing validity of attributes and customers. The owner generating the tree of signs and sends it directly to the server of the cloud. The customers encode the files and sign them, after that upload them to the cloud server. By then the server authenticates the sign of the documents, if the approval is effective, simply the customers get read and write access of the reports and the cloud server stores the altered documents.

2.4 Access Control Scheme in PUD

2.4.1 Scheme Design

In the public domain, an enormous number of consumers, a few attributes possessed by the client, difficulty management, and undefined clients' identity. Based on the above characteristics, the user has the right access only to read.

Although the CP-ABE can attain access rule, it cannot satisfy the needs of complex cloud architecture. In previous CP-ABE, the management of attributes and distribution of keys is accomplished by only one authorized agency. The owner specifies access rights and files were encrypted in accordance with this access right. Key is distributed to all users depending on his rights. If the users satisfy attributes in the access plan then he can decode the information. Although, in case of there is just one expert in the system then he circulated all the keys.

Basically, there are two issues will show up in the application:

- In the cloud condition, there are a few experts and every expert in their individual field manages some parts of consumers' attributes. The consumer claimed attributes get from various experts.
- The allocation of all the keys is given by one expert when there is just a single trusted expert.

The usual interface between the consumer and trusted expert cannot just bring blockage for the framework load capacity, yet in addition upgrades the potential security hazards. Along these lines, Multi-Authority ABE (MA-ABE) is utilized in this project.

In public platform, owner does not have any information about users directly. At first, owner encrypts the files and transfer to cloud server. After approval, the particular decoding key received by the owner and gets the access request of document through the cloud server. At that point consumers can utilize their own decoding key to decode the encoded information, after the cloud server send back the encoded information. The work process of this area is illustrated in Figure 3.

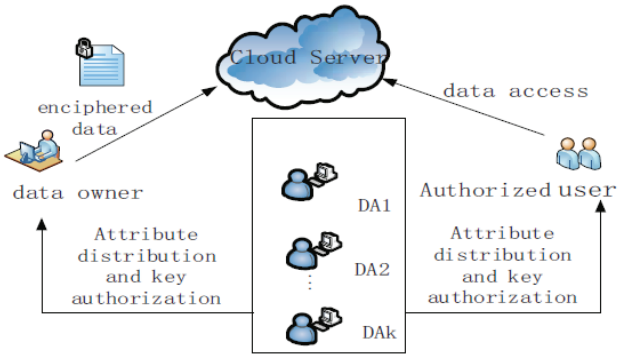

Figure 3. Access control framework of PUD.

2.4.2 Access Control Process

From the above investigation, we utilize a HABE to execute better accessing in the open platform.

- Files creation: The creating of documents is ended through the owner. All in all, to protect the order of the data, the owner initially encodes data and after that stores it in the cloud. To minimize the cipher text size and complexity design, the owner joins the symmetric encoding plot with a public key encryption conspire. The way toward making a document is demonstrated as follows:
- Select a unique *ID* for the file.
- Choose a random symmetric encoded key $\overset{R}{\leftarrow} K$. *K* means key space, and encodes the information file with *CK*.
- Define access tree T, utilize the algorithm $HABE.Encrypt(PK_e, CK, T)$ to encode *CK* and go back the *CT*.
- The owner creates the CT by hash undertakings and signs h(CT) to get the sign SG, not only to give the decency of the data yet, furthermore but also to encourage the cloud and customer to support the data owner identity.
- Data access: if the customer needs to get appropriate files, he ought to get the documents from the cloud server and after that decode the data, which correlated to the decoding procedure. There are two segments: firstly utilize the algorithm *HABE Encrypt* (PK_e, *CK, T)* to decrypt the symmetric encoded key *CK*, then utilize the key *CK* to decode the file.
- Files remove: if the owner needs to erase a document, he can dispatch the ID of the file and sign SG to the cloud server; at that point the server erases the records subsequent to confirming the owner's sign.
- Attribute revocation: Depending on the customers' request the authors allocates attributes to each customer and accomplices the set of attributes by lapse time T. The access structure attributes encase a time attribute *T* ', if *T* >*T*' then the attributes are equal, then this file can be right to use. So the owner can control users' permissions by changing the time attributes.
- Users' attributes Revocation: The Data Access calculates the least amount of attributes A_{min} that allows customers' permission rejection, and $A_{new} = A\text{-}A_{min}$ *new*, making $T(A_{min})$ returns null. Set new lapse time each attribute set, makes new private key components and return it to the client.

3. Results And Analysis

3.1 Security Analysis

In private platform, the customer will get well the records contrasting with the aggregate keys and do not offer access to various reports in the personal domain, so the owner controls the customers' permission set. The sign strategy is defined by the owner and sent explicitly to the cloud server. The CA does not know the sign assertion. So the CA cannot control the information without leak to any other person. Thus, the write rights still have a place with the owner. In this methodology, the customers' ID and the sign is simply compared to the customers' attributes, so the customer's attributes are secured. All in all, the IABS plan can guarantee customers' security.

In a public platform, the HABE plot for the different number of customers with the temporary identity in this platform. For the trustworthy CA, it will issue the private key and the corresponding attribute structure with the expert in the fundamental measurement not to the customers, from now on the CA does not directly control the private key of the customer's, along these lines sinking the trust in CA.

3.2 Simulation Analysis

In our KAE procedure in the personal domain, the parameters of the framework are made by the expert, which is not inside our idea. In further, the $\hat{e}(g_1, g_n)$ can be discovered in the framework setup. Furthermore, the aggregate key simply needs one matching action, and to process a combining task is fast, the specific evaluation can be illustrated in Figure 4.

In Figure 4, the Attribute-based Encryption algorithm of MAH-ABE strategy invested more time than the KAE calculation utilized in our plan. The recreation results portray the higher efficiency of the plan.

In Figure 5, the client just requires lesser time to sign the changed documents. While, the endorsement time just makes up a little part, so the methodology of signature and confirmation use a less time. Along these lines, from the client's point of view, our scheme is efficient.

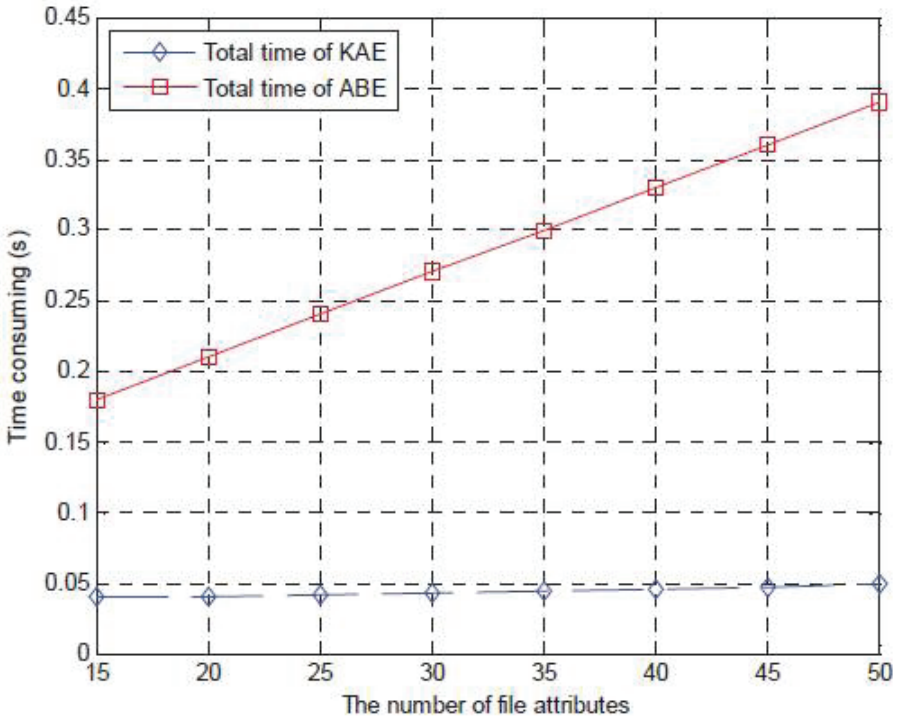

Figure 4. Total time of KAE and ABE.

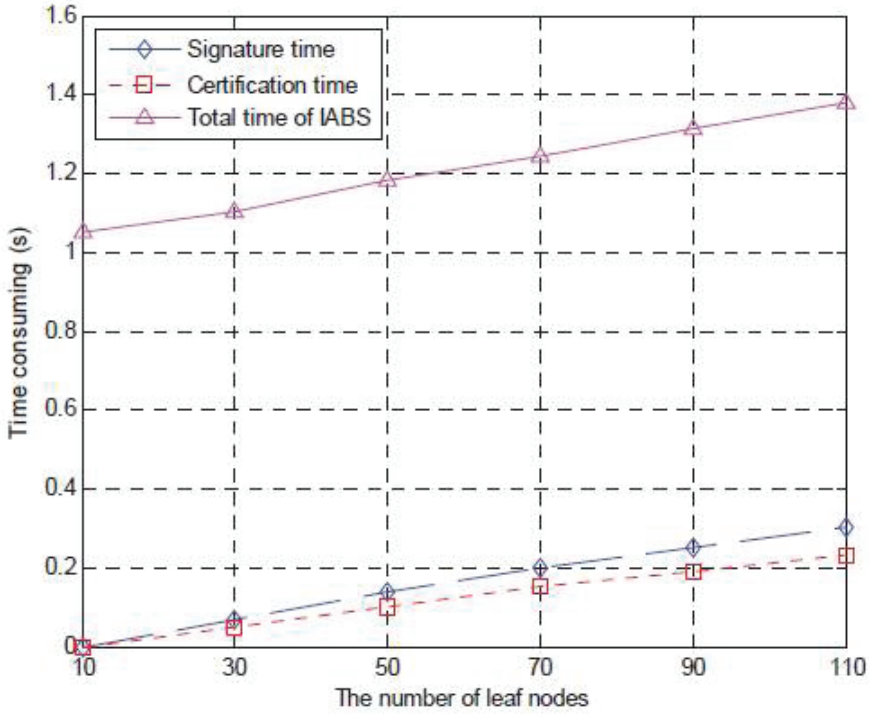

Figure 5. The signature and authentication time of IABS.

4. Conclusion

This study shows new privacy preserving access control scheme utilizing KAE and IABE algorithms to deal with the access privileges of the clients and ensure the clients identity protection in private and public platforms. Utilizing the KAE enhance the effectiveness in overseeing client's access right in private domain. Utilizing the IABE algorithm to uphold read and write privileges of clients in the private domain effectively and protect the privacy of the user's identity. To keep away from single point of failures in the public platform we utilize HABE scheme and achieve information sharing viably. By contrasting the MAH-ABE scheme, the proposed plan demonstrates the practicability and better to protect the security of information in cloud-based services.

5. References

1. Yu S, Wang C, Ren K. Achieving secure, scalable, and fine-grained data access control in cloud computing. Proceedings IEEE INFOCOM. 2010; p. 1–9. https://doi.org/10.1109/INFCOM.2010.5462174
2. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. IEEE Symposium on Security and Privacy (SP '07). 2007; p. 321–34. https://doi.org/10.1109/SP.2007.11
3. Hur J, Noh DK. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems. 2011; 22(7):1214–21. https://doi.org/10.1109/TPDS.2010.203
4. Lewko A, Waters B. Decentralizing attribute-Based encryption. Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2011; p. 568–88. https://doi.org/10.1007/978-3-642-20465-4_31
5. Li M, Yu S, Zheng Y. Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encryption. IEEE Transactions on Parallel and Distributed System. 2013; 24(1):131–43. https://doi.org/10.1109/TPDS.2012.97
6. Chu CK, Chow SSM, Tzeng WG. Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Transactions on Parallel and Distributed Systems. 2014; 25(2):468–77. https://doi.org/10.1109/TPDS.2013.112
7. Li J, Kim K. Hidden attribute-based signatures without anonymity revocation. Information Sciences. 2010; 180(9):1681–9. https://doi.org/10.1016/j.ins.2010.01.008
8. Kumar S, Agrawal S, Balaraman S. Attribute based signatures for bounded multi-level threshold circuits. European Public Key Infrastructure Workshop. 2011; p. 141–54. https://doi.org/10.1007/978-3-642-22633-5_10