SECURITY INSURANCE BASED ACCESS CONTROL CONSPIRE IN CLOUD-BASED ADMINISTRATIONS

Amara naga venkata supraja [1], M. Lakshmi Bai [2]

[1] M. Tech Research scholar, St. Ann's College of Engineering & Technology, Chirala
[2]Assoc. Professor, Department of Computer Science and Engineering, St. Ann's College of Engineering & Technology, Chirala.

amarasupraja01@gmail.com , lakshmimaddala81@gmail.com

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: access control; data sharing; privacy protection; cloud-based services

I. INTRODUCTION

In the advancement of cloud computing, big data and public cloud services have been used in all applications. The data can be stored securely in cloud server by users. Cloud computing is easily available to all users and enterprises. In cloud we can protect data more efficiently by transferring data over the internet to the offsite cloud storage system.

Access control is a security technique that regulates the use of resources and reduces risk of business or organizations. There are two types of access controls physical and logical. Physical access control is access to buildings, rooms and campuses. Logical access control

connects to computer networks, system files and data. Access control system performs identification and authorization of users by evaluating login credentials such as passwords, personal identification numbers and security tokens etc.

Security is a major problem in cloud computing. For this we need to develop an efficient access control system.

In this project, we present a more systematic, flexible and efficient access control scheme. The following main contributions are:

1. We propose an access control system called PSACS, which is privilege separation based on privacy protection. The system uses Key-Aggregate Encryption (KAE) scheme and Hierarchy Attribute-based Encryption (HABE) scheme to implement read access control scheme in the PSD and PUD respectively. The KAE scheme greatly improves access efficiency and the HABE scheme largely reduces the task of a single authority and protects the privacy of user data.

2. Compared with the MAH-ABE scheme which does not refer to the write access control, we exploit an Improved Attribute-based Signature (IABS) scheme to enforce write access control in the PSD. 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 a thorough analysis of security and Complexity 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. EXISTING SYSTEM

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. Data sharing is an important functionality in cloud storage. We show how to securely, efficiently, and flexibly share data with others in cloud storage. Describe new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights [7] for any set of cipher texts are possible. Data sharing scheme based on systemic attribute encryption, which endows different users' different access rights. But it is not efficient from the complexity and efficiency.

2.1 Disadvantages of Existing System

1. The traditional access control strategy cannot effectively solve the security problems that exist in data sharing.
2. This scheme does not consider the revocation of access permissions.
3. It can easily cause key escrow issue.

III. PROPOSED WORK

We propose a novel access control system called PSACS, which is privilege separation based on privacy protection. The system uses Key-Aggregate Encryption (KAE) scheme and Hierarchy Attribute-based Encryption (HABE) scheme to implement read access control scheme in the PSD and PUD respectively.

The KAE scheme greatly improves access efficiency and the HABE scheme largely reduces the task of a single authority and protects the privacy of user data. Compared with the MAH-ABE scheme which does not refer to the write access control, we exploit an Improved Attribute-based Signature (IABS) scheme to enforce write access control in the PSD. In this way, the user can pass the cloud server's signature verification without disclosing the identity, and successfully modify the file.

3.1 Advantages of proposed System

1. In this project, we present a more systematic, flexible and efficient access control scheme.
2. We provide a thorough analysis of security and complexity 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.
3. The evaluation results show the high efficiency of our scheme

IV. PROPOSED FRAMEWORK

Global Setup( ). The Global Setup algorithm takes as inputs a security parameter and universe description *U*. Let G1,G2, and Gt be the multiplicative groups with the same prime order *p*, and e:G1*G2→Gt be the bilinear map. Let g1be the generator G1 of and g2 be the

generator of G2 . Let H:{0,1}*→G2 be a hash function such that the security will be modeled in the random oracle.

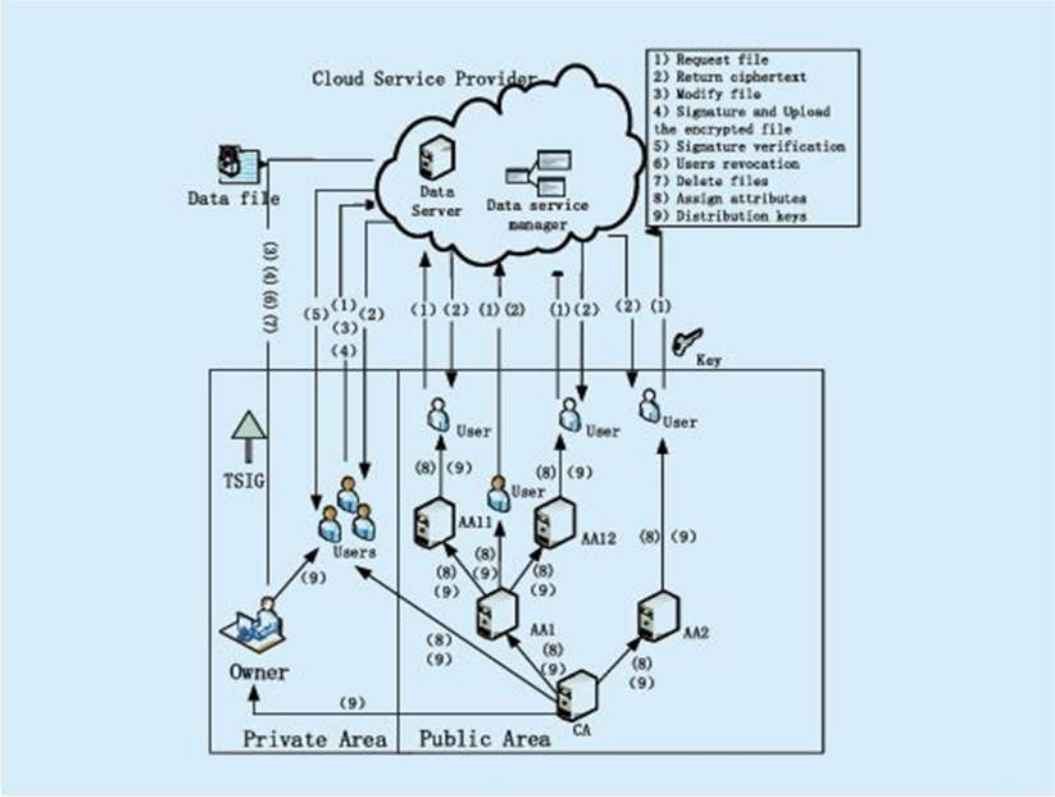


Fig 3.2 System framework

4Analysis

In this we propose security analysis and performance analysis of access control scheme.

4.1 Security analysis

In PRD, users can only decrypt the files corresponding to the received aggregate keys and do not have access to other files, thus the data owner controls the users' access permissions. When the data file is modified, although CA is trusted, the system parameters and revocation instructions are generated by the CA. The signature policy is formulated by the data owner and is sent directly to the cloud server. The CA does not know the signature policy. Assuming that CA cannot give itself authorization, as long as the attributes of CA cannot satisfy the access policy, it is not valid to modify the file. Thus, the write access

permissions still belong to the data owner. In the process of the users' signature, the signature key is only related to the users' attributes, so the user's identity is secure.

In PUD, our construction achieves data confidentially. The outsourced data can be confidential against a user whose attributes do not satisfy the access policy. Since the attributes cannot satisfy the access structure in the cipher text, the user cannot receive the partially decrypted cipher text during the transformation process. Thus, he cannot recover the original message.

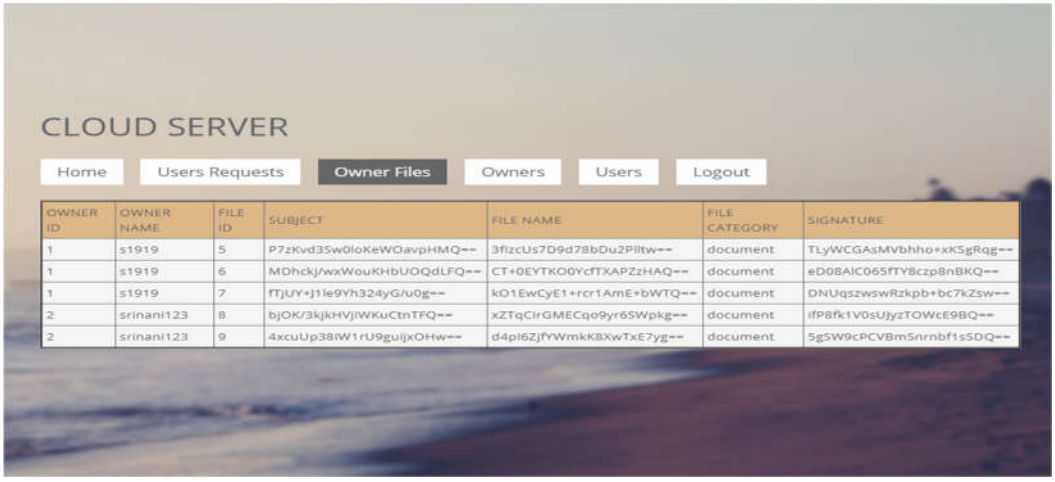
4.2 Performance analysis

In our KAE scheme in the PRD, the system parameters are generated by the trusted authority, which is not within our consideration. Moreover e(g1,gn) can be calculated in the system setup phase. In addition, the aggregate key only needs one pairing operation, and to calculate a pairing operation is very fast, the specific comparison.

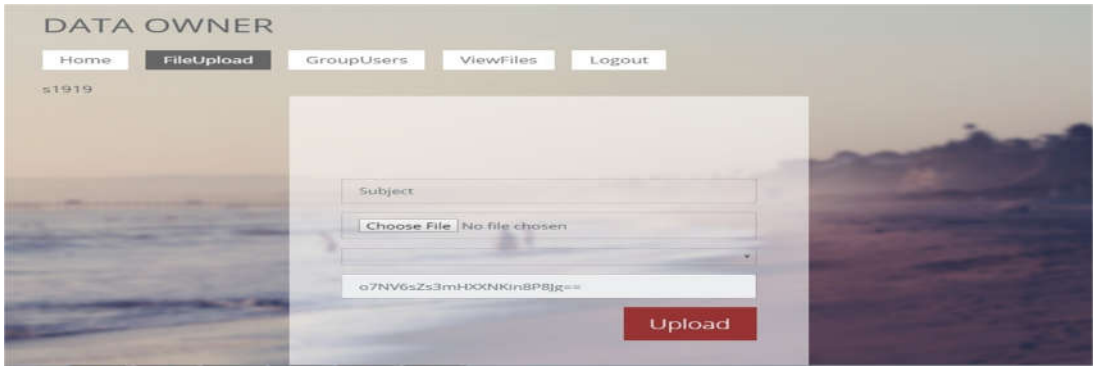
The attribute-based encryption algorithm of the MAH-ABE scheme spent much more time than the KAE algorithm used in our scheme. If the attribute revocation occurs, the ABE algorithm will be more time-consuming. More importantly, the growth rate of time spent with the number of file attributes is much higher than KAE algorithm. The user only needs a very short time to sign the modified files. While, the authentication time only makes up a small part, so the process of signature and authentication consume a very small time. Therefore, from the client's perspective, the program is efficient.

In PUD, we adopt outsourcing decryption method. We compare our scheme with Ruji's Scheme. We compared the computing time incurred in encryption and decryption. the number of authorities is set to 10. It is obvious that our scheme requires less time for encryption and decryption than Ruji's scheme, especially for decryption. Since in the decryption phase, major computation overhead is delegated to the cloud, user only needs one exponentiation operation to recover the original message. Therefore, the decryption time for users can be greatly reduced. Computing cost for transformation. On the whole, it can be concluded that our scheme's computation efficiency is much better than Ruji's scheme.

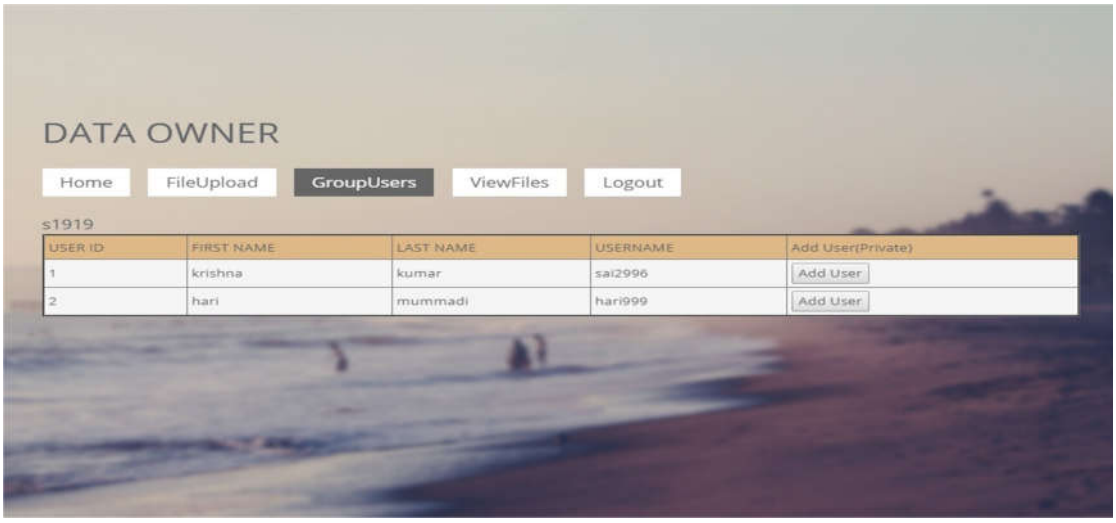
V. SCREEN SHOTS



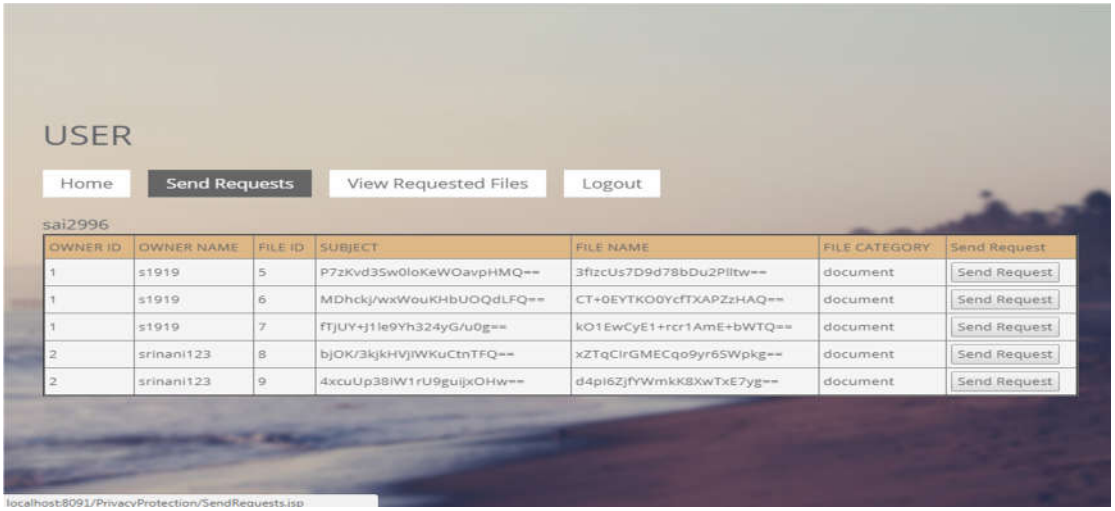
CS_ Owner files



Data Owner file upload



Group Users



User Requests

VI. CONCLUSION

In this project, to protect user's data and to store securely in cloud we can propose an access control scheme (PS-ACS). Access control can reduce the risk of many organizations and keep more security to the data. So we can implement access control scheme based on privilege separation. In this scheme we can divide users in to private domain and public domain.

In this project data owner related to the private domain so the data owner can access both read and write permissions. Users are related to the public domain they can access only read permissions. To access write permissions add the users to the public domain then they

can download and modify the files. Data owner sends access keys to the cloud authority. After obtaining key it can authorizes owners and users then data owners encrypt their files by using corresponding encryption (KAE). Data owner sends and shares secret keys to the server to download and view the files and stored them in cloud based services. Compared to the MAH-ABE scheme, the proposed scheme shows the feasibility and improves more efficiency to protect the privacy of data in cloud-based services.

VII. FUTURE ENHANCEMENT

Cloud computing brings awesome accommodation for individuals. Especially, it flawlessly coordinates the expanded need of sharing information over the Internet. In future Cloud computing users are identified and used their identities for accessing the services. A secure trust based identity management scheme is essentially a need by all cloud service provider and users. Various issues of identity management system are identified.

VIII. 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, "Cipher text-policy attribute-based encryption," Proc. Security and Privacy, pp. 321-334, 2007.

[3] M. Chase. Multi-authority attribute-based encryption. In (To Appear) The Fourth Theory of Cryptography Conference (TCC 2007), 2007

[4] 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.

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

[6] 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.

[7] 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.

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

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

[10] 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.

[11]A. Sahai and B. Waters. Fuzzy Identity Based Encryption. In Advances in Cryptology – Euro crypt, volume3494 of LNCS, pages 457–473. Springer, 2005.

[12] BETHENCOURT J, SAHAI A, WATERS B, "Cipher text- Policy Attribute-based Encryption", *IEEE Symposium on Security and Privacy*, vol. 2008,no. 4, pp. 321-334, 2007.

[13] ATTRAPADUNG N, IMAI H, "Conjunctive Broadcast and Attribute-Based Encryption", *Proceedings of Pairing-based Cryptography – Pairing2009*, vol. 5671, pp. 248-265, 2009.

[14] ATTRAPADUNG N, IMAI H, "Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes", *Proceedings of Cryptography and Coding 2009*, pp. 278-300, 2009.

[15] HUR J, NOH D K, "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.

[16] LEWKO A, WATERS B, "Decentralizing Attribute-based Encryption", *Proceedings of Advances in Cryptology-EUROCRYPT 2011 - 30th*th*Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 568-588, 2011.

[17] LI M, YU SH, ZHENG Y, "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.

[18] XIE X, MA H, LI J, et al, "New Cipher text-Policy Attribute-based Access Control with Efficient Revocation", *Proceedings of* Information and Communication Technology 2013.

[19] LIANG K, MAN H A, SUSILO W, et al, “An Adaptively CCA-Secure Cipher text-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing”, *Information Security Practice and Experience*, pp. 448-461, 2014.

[20] CHEN D, SHAO J, FAN X, “MAH-ABE based Privacy Access Control in Cloud Computing”,*Chinese Journal of Electronics*, vol. 42, no. 4, pp. 821-827, 2014.

[21] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Attribute Based Systems. InACM conference on Computer and Communications Security(ACM CCS), 2006.

[22] LI J, KIM K, “Hidden Attribute-based Signatures without Anonymity Revocation”, *Information Sciences*, vol. 180, no. 9, pp. 1681-1689, 2010.

[23] NARAYAN S, GAGNÉ M, SAFAVI-NAINI R, “Privacy Preserving EHR System Using Attribute-based Infrastructure”, *Proceedings of ACM Cloud Computing Security Workshop 2010*, pp. 47-52, 2010.

M. Lakshmi Bai,

Associate Professor in CSE department in St.Ann`s College of engineering and technology having 14 yrs of experience .Research areas of interest in Data Mining, Recommender System, and Computer Networks.

Name:-A.N.V. Supraja

Department: - Computer Science and Engineering

Project Title:-Security Insurance based access control conspire in cloud based administrations.

College Name: - St.Ann`s college of engineering and technology

Email-id: amarasupraja01@gmail.com

Mobile no: - 9010965955

Address: - Andhra bank bazaar

Uppugundur, Prakasam

Pincode:-523186

About me:- M.Tech in computer science and engineering at St. Ann’s college of engineering and technology which is affiliated under jntu Kakinada. My area of interest is Programming Languages.