Privacy Protection Based Access Control Scheme In Cloud-Based Services

Tippareddy Jahnnavi Reddy , Miss G.Keerthana, Sri.V.Bhaskara Murthy
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

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.

I. INTRODUCTION

With the rapid development of cloud computing, big dataand public cloud services have been widely used. The user canstore his data in the cloud service. Although cloud computingbrings great convenience to enterprises and users, the cloudcomputing 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. Therefore, we need to developan effective access control solution. Since the traditional accesscontrol strategy [1] cannot effectively solve the securityproblems that exist in data sharing. Data security issuesbrought by data sharing have seriously hindered thedevelopment of cloud computing, various solutions to achieveencryption and decryption of data sharing have been proposed.

In 2007, Bethencourt et al. [2] first proposed the ciphertextpolicy attribute-based encryption (CP-ABE). However, thisscheme does not consider the revocation of access permissions.

In 2011, Hur et al. [3] put forward a fine-grained revocationscheme but it can easily cause key escrow issue. Lewko et al. [4] used multi authority ABE (MA-ABE) to solve key escrowissue. But the access policy is not flexible. Li et al [5]presented data sharing scheme based on systemic attributeencryption, which endows different users' different accessrights. But it is not efficient from the complexity and efficiency.

In 2014, Chen et al. [6] proposed Key-Aggregate Encryptionalgorithm, effectively shortening the length of the ciphertextand the key, but only for the situation where the data ownerknows the user's identity. These schemes above only focus onone aspect of the research, and do not have a strict uniformstandards either. In this paper, we

present a more systematic,flexible and efficient access control scheme. To this end, wemake the following main contributions:

1. We propose a novel access control system called PSACS,which is privilege separation based on privacy protection.The system uses Key-Aggregate Encryption (KAE) schemeand Hierarchy Attribute-based Encryption (HABE) scheme toimplement read access control scheme in the PSD and PUDrespectively. The KAE scheme greatly improves accessefficiency and the HABE scheme largely reduces the task of asingle authority and protects the privacy of user data.

2. Compared with the MAH-ABE scheme which does notrefer to the write access control, we exploit an ImprovedAttribute-based Signature (IABS) [7-9] scheme to enforcewrite access control in the PSD. In this way, the user can passthe cloud server's signature verification without disclosing theidentity, and successfully modify the file.

3. We provide a thorough analysis of security andcomplexity of our proposed PS-ACS scheme. The functionalityand simulation results provide data security in acceptableperformance impact, and prove the feasibility of the scheme.

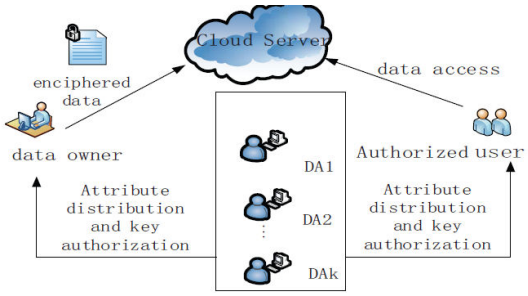
II. EXISTING SYSTEM

- The trait based access control empowers information distributors to characterize information get to approaches without knowing what number of clients in the framework previously.
- The most critical preferred standpoint is that just a single duplicate of the scrambled information is created in attribute-based get to control. Since ABE can be utilized to ensure information security, naturally it can likewise be connected to ensure membership security.
- A clear strategy is to scramble membership trapdoor by utilizing ABE with another arrangement of parameters. In any case, this technique requires the expert, who is in charge of quality administration and key age in an ABE framework, to create labels for each distributed information or trapdoors for every datum endorser.

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.

IV. SYSTEM ARCHITECTURE



V. MODULES

Data owner

In this module, data owner has to register to Authentication Center and Authentication Center checks and authorizes the data owner login . Data owner browse the file , encrypt and upload file with its mac. Once uploaded the file all the authentication center must provide the storage access for the file store on the cloud.

Data owner can also delete the file after the uploading of the file to the cloud.

Authentication Center
In this module Authentication Center checks user & owner login and authorizes the registration. Authentication center list all other sub-authentication centers and provide authorization (Activate OR Deactivate). Authentication center provides the storage access to cloud for every file uploaded by the data owner.

Sub - Authentication Center 1
In this module the authentication center 1 shows all the private key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

Sub - Authentication Center 2
In this module the authentication center 2 shows all the public key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

Cloud Server
Receive all files from the data owner and store all files, user details. Provide files to end user after verifying Private key and secret key provided by the authentication center. Maintain file transaction details and forward the file download request from the user to the authentication centre.

End User (Receiver)
In this module end user has to register and login, and the user is authorized by the authentication center, user will request private key from the sub-authentication center1 and the secret key from the sub-authentication center2 to download the file from cloud server.

VI. 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 thecharacteristics of the user, we divide the users into personaldomain (PSD) and public domain(PUD) logically. In the PSD,the KAE algorithm is applied to implement users read accesspermissions and greatly improved efficiency. The IABSscheme is employed to achieve the write permissions and theseparation of read and write permissions to protect the privacyof the user's identity. In the PUD, we use the HABE scheme toavoid the issues of single point of failure and to achieve datasharing. Furthermore, the paper analyzes the scheme fromsecurity and efficiency, and the simulation results are given. Bycomparing with the MAH-ABE scheme, the proposed schemeshows the feasibility and superiority to protect the privacy ofdata in cloud-based services.

REFERENCES

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

[2] J. Bethencourt, A. Sahai, B. Waters, “Ciphertext-policy attribute-basedencryption,” Proc. Security and Privacy, pp. 321-334, 2007.

[3] J. Hur, D.K. Noh, “Attribute-based access control with efficientrevocation in data outsourcing systems,” IEEE Transactions on Paralleland 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 healthrecords in cloud computing using attribute-Based Encryption,” IEEETransactions 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 forscalable data sharing in cloud storage,” IEEE Transactions on Paralleland Distributed Systems, vol. 25, no. 2, pp.468-477, 2014.

[7] J. Li, K. Kim, “Hidden attribute-based signatures without anonymityrevocation,” 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 forbounded multi-level threshold circuits,” Proc. Public Key Infrastructures,Services and Applications, pp. 141-154, 2011.