Privacy Protection Based Access Control Scheme in cloud-Based Services

Chinnam Prudhvi Raju [1], M.Naresh [2]

[1]*Pursuing M.Tech (software engineering), Newton's Institute of Engineering College, Alugurajupally, macherla, Guntur dist, AP, India*

[2]*Associate Professor,Newton's Institute of Engineering College, Alugurajupally, macherla, Guntur dist, AP, India*

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 cipher text 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.**

I. INTRODUCTION

With the rapid development of cloud computing, big data and public cloud services have been widely used. 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. Therefore, we need to develop an effective access control solution. Since the traditional access control strategy [1] cannot effectively solve the security problems that exist in 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 escrow issue. But the access policy is not flexible. Li et al [5] presented 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. In 2014, Chen et al. [6] 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. These schemes above only focus on one aspect of the research, and do not have a strict uniform standards either.

II. LITERATURE SURVEY

2.1 Introduction

Literature Survey is the most important step in software program development manner. Before growing the tool it's miles necessary to decide the time thing, financial system n employer strength. Once these things are glad, ten subsequent steps are to determine which working device and language may be used for growing the tool. And language can be used for developing the tool. Once The programmers begin constructing the tool the programmers want lot of outside guide. This aid can be acquired from senior programmers, from e-book or from web sites. Before constructing the gadget the above attention r taken under consideration for developing the proposed device.the proposed system.

Literature survey Is the documentation of a comprehensive assessment of the published and unpublished work from secondary resources statistics inside the regions of particular interest to the researcher. The library is a wealthy storage base for secondary facts and researchers used to spend numerous weeks and sometimes months going through books, journals, newspapers, magazines, convention lawsuits, doctoral dissertations, grasp's theses, authorities guides and financial reports to locate statistics on their research topic.

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.
- In 2007, Bettencourt et al. first proposed the cipher text policy attribute-based encryption (CP-ABE).
- Li et al presented 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.
- Chen et al. 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.

DISADVANTAGES OF EXISTING SYSTEM:

- The traditional access control strategy cannot effectively solve the security problems that exist in data sharing.
- This scheme does not consider the revocation of access permissions.
- It can easily cause key escrow issue.
- These existing schemes only focus on one aspect of the research, and do not have a strict uniform standards either.

2.3 PROPOSED SYSTEM:

PROPOSED SYSTEM:

- 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.

ADVANTAGES OF PROPOSED SYSTEM:

- In this paper, we present a more systematic, flexible and efficient access control scheme.
- 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.
- The evaluation results show the high efficiency of our scheme.

III. SYSTEM DESIGN

3.1 Introduction

Designing is the most important phase. The Design process involves developing a conceptual view of the system, establishing system structure, identifying data string and data stores, decomposing high level functions into sub-functions, establishing relationships, interconnections among components and developing concrete data representation.

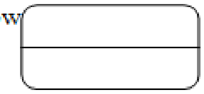
3.2 DFD / ER / UML diagram

DFD SYMBOLS:

In the DFD, there are four symbols

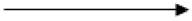
1. A square defines a source (originally) or destination of system data.
2. An arrow identifies data flow. It is the pipe line through which the information flows.
3. A circle or a bubble represents a technique that transforms profits statistics flow into outgoing data flows.
4. An open rectangle is a data store, data at rest or a temporary repository of data.

Process that transforms data flow



Process that transfer data flow

Data flow

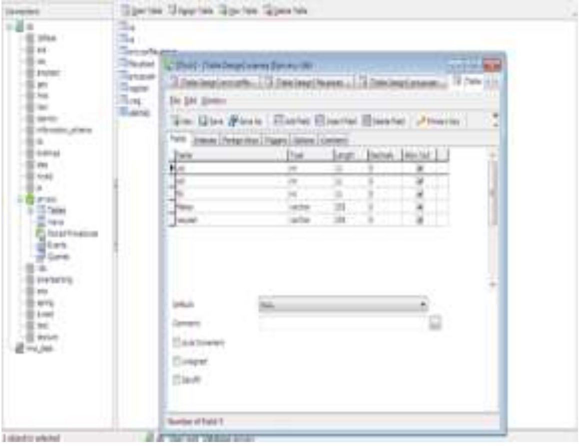


Data Store

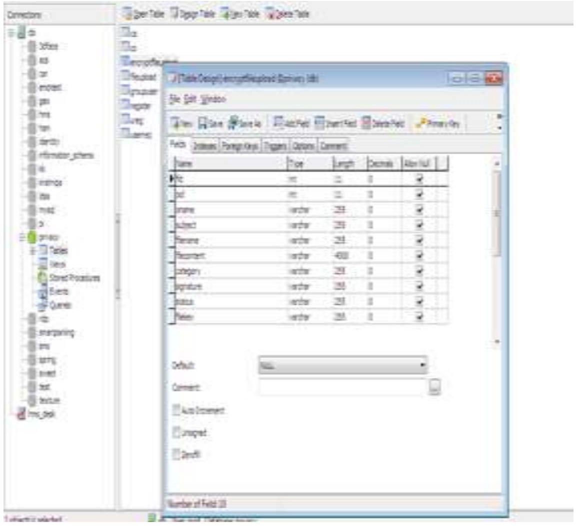
The development of DFD'S is done in several levels. Each process on lower level diagrams can be broken down into a more detailed DFD in the next level.

DATABASE SCREENSHOTS:

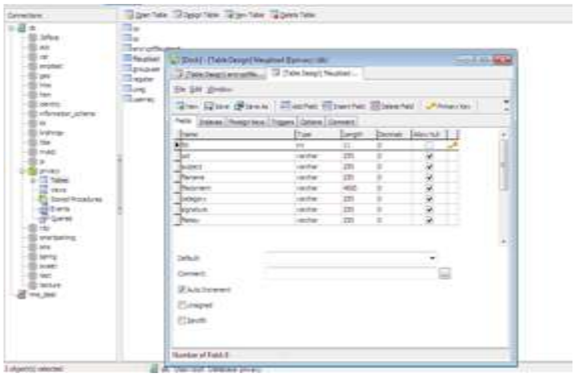
User Requests:



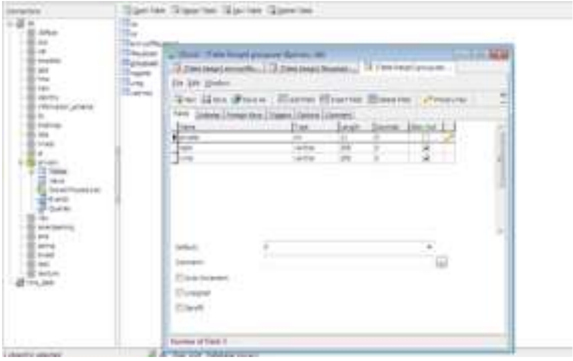
Encrypted file details:



Uploaded files:

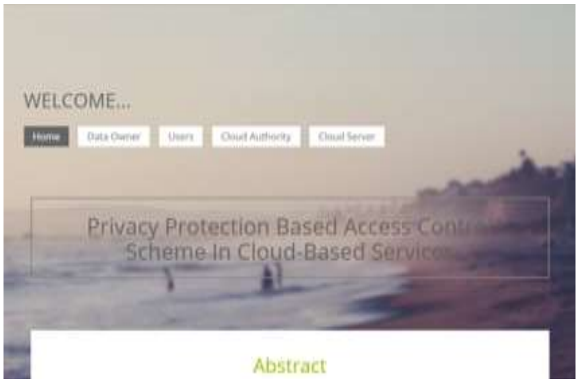


Grouping users:

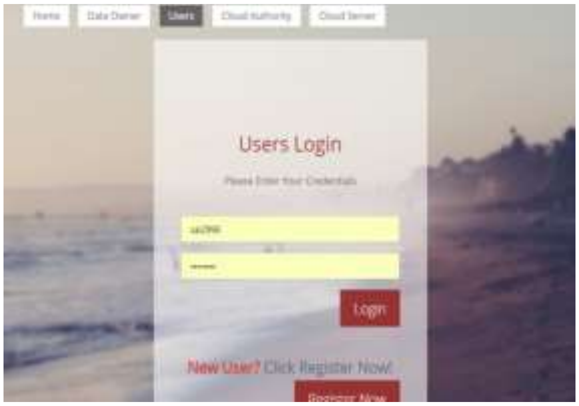


IV. OUTPUT SCREEN

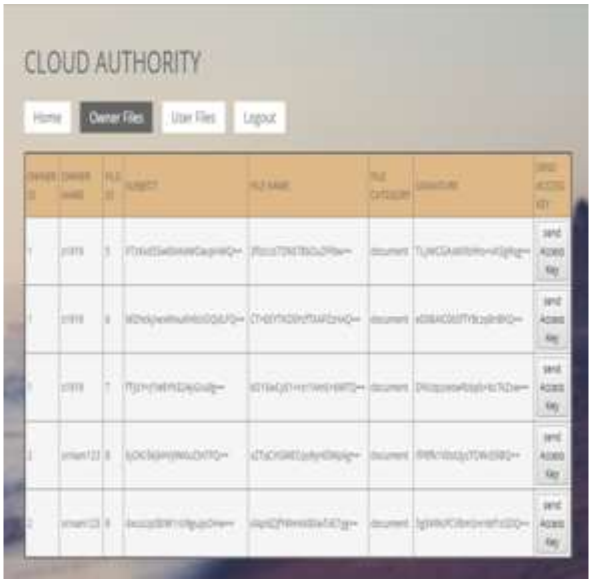
Homepage:


WELCOME...
Home
Data Owner
Users
Cloud Authority
Cloud Server
Privacy Protection Based Access Contr
Scheme In Cloud-Based Service
Abstract

User login page:

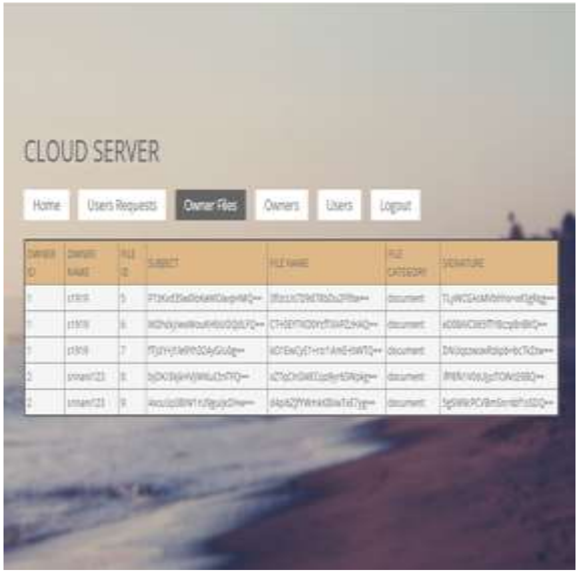


CA_Ownerfiles :



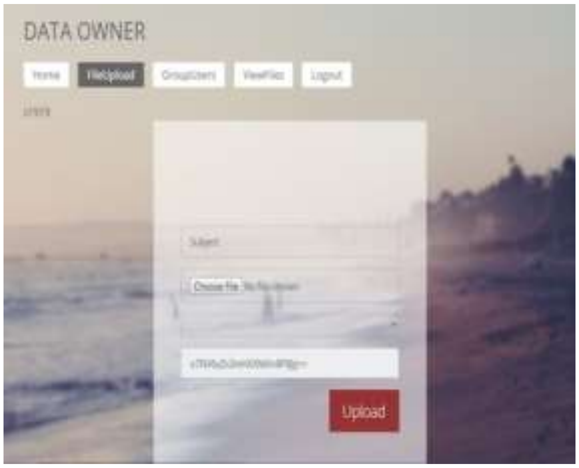
OWNER ID	OWNER NAME	FILE ID	SUBJECT	FILE NAME	FILE CATEGORY	SIGNATURE	SEND ACCESS KEY
1	ct919	5	[illegible]	[illegible]	document	[illegible]	Send Access Key
1	ct919	6	[illegible]	[illegible]	document	[illegible]	Send Access Key
1	ct919	7	[illegible]	[illegible]	document	[illegible]	Send Access Key
2	sriram123	8	[illegible]	[illegible]	document	[illegible]	Send Access Key
2	sriram123	9	[illegible]	[illegible]	document	[illegible]	Send Access Key

CS_Ownerfiles:

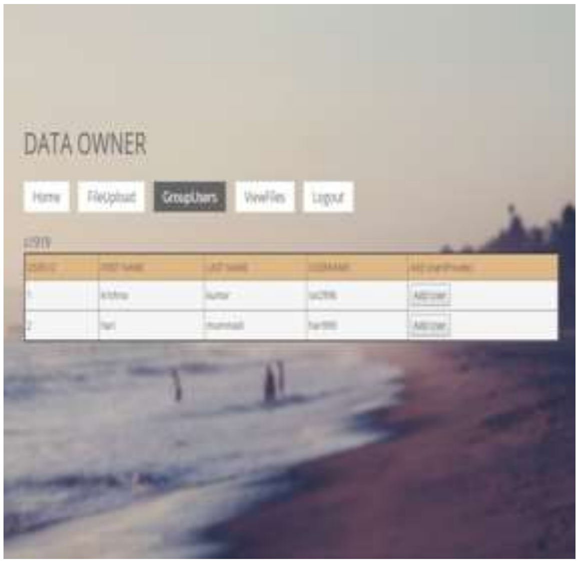


OWNER ID	OWNER NAME	FILE ID	SUBJECT	FILE NAME	FILE CATEGORY	SIGNATURE
1	ct919	5	[illegible]	[illegible]	document	[illegible]
1	ct919	6	[illegible]	[illegible]	document	[illegible]
1	ct919	7	[illegible]	[illegible]	document	[illegible]
2	sriram123	8	[illegible]	[illegible]	document	[illegible]
2	sriram123	9	[illegible]	[illegible]	document	[illegible]

DataOwner_Fileupload:

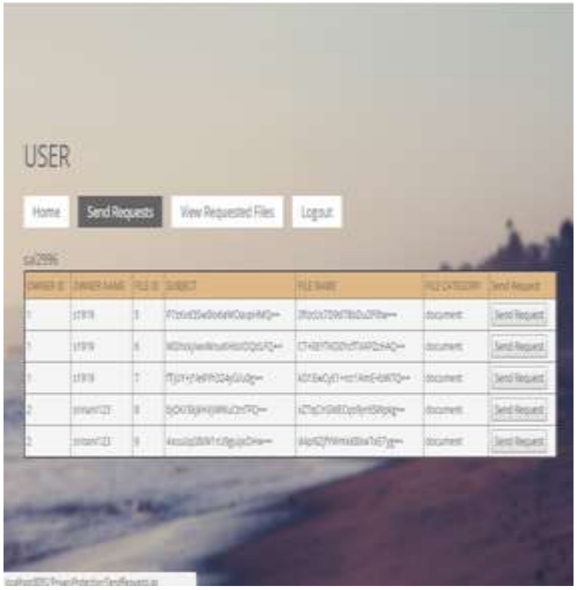


GroupUsers:



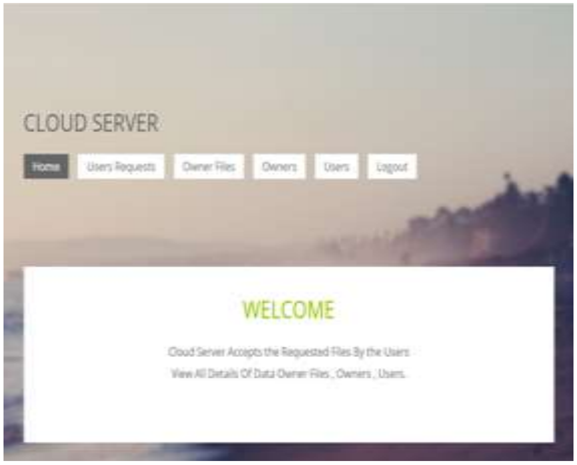
USER ID	FIRST NAME	LAST NAME	USERNAME	ADD USER/PRIVATE
1	krishna	kumar	sai2996	Add User
2	hari	murmadi	hari999	Add User

User Requests:



OWNER ID	OWNER NAME	FILE ID	SUBJECT	FILE NAME	FILE CATEGORY	Send Request
1	ct919	5	[illegible]	[illegible]	document	Send Request
1	ct919	6	[illegible]	[illegible]	document	Send Request
1	ct919	7	[illegible]	[illegible]	document	Send Request
2	sriram123	8	[illegible]	[illegible]	document	Send Request
2	sriram123	9	[illegible]	[illegible]	document	Send Request

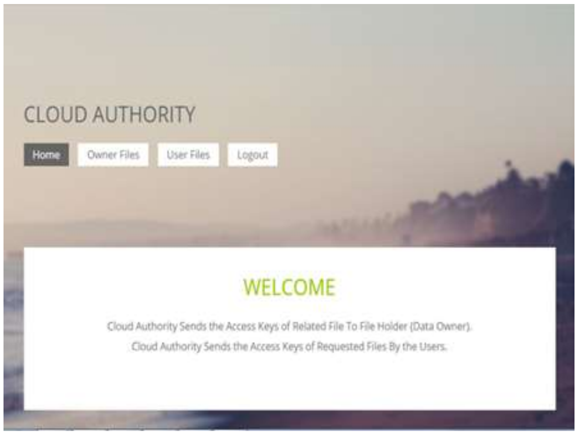
CS_Home:



Cloud Server Accepts the Requested Files By the Users

View All Details Of Data Owner Files , Owners , Users.

CA_Home:



WELCOME

Cloud Authority Sends the Access Keys of Related File To File Holder (Data Owner).
Cloud Authority Sends the Access Keys of Requested Files By the Users.

V. 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 user, we divide the users into personal domain (PSD) and public domain(PUD) logically. In the PSD, the KAE algorithm is applied to implement users 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 user's identity. In the PUD, we use the HABE scheme to avoid the issues of single point of failure and to achieve data sharing. Furthermore, the paper analyzes the scheme from security and efficiency, and the simulation results are given. 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.

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.