Journal of Engineering Sciences

Vol 11, Issue 7,July/2020

ISSN NO:0377-9254

Privacy Protection based Access Control Scheme in Cloud-based Services

B SEVA NAIK[1], ABDULLAH SHAREEF[2]

[1] Assistant Professor, Dept of CSE, Mahaveer Institute of Science and Technology, Hyderabad, TS, India , E-MAIL: sevanaikb@gmail.com

[2] PG Scholar, Dept of CSE, Mahaveer Institute of Science and Technology, Hyderabad, TS, India , E-MAIL: shareefabdullah1122@gmail.com

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 cipher text 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: Key-Aggregate Encryption (KAE), Attribute-based Signature (IBS), cipher text, Cloud.

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 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. first proposed the ciphertext policy attribute-based encryption (CP-ABE). However, this scheme does not consider the revocation of access permissions. In 2011, Hur et al. put forward a fine-grained revocation scheme but it can easily cause key escrow issue. Lewko et al. used multi authority ABE (MA-ABE) to solve key escrow issue. But the access policy is not flexible. 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.

In 2014, 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. These schemes above only focus on one aspect of the research, and do not have a strict uniform standards 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 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.
2. Compared with the MAH-ABE scheme which does not refer to the write access control, we exploit

an Improved Attribute-based Signature (IABS) [7-9] 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:

- 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.

- 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.

MODULE DESCRIPTION

Data Owner: 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.

Personal domain (PSD), in which users have special privileges, such as family, personal assistant, close friends and partners. This domain has a small number of users and small scale attributes, and the data owner knows the user's identity, which is easy to manage.

Data 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 send to the cloud server. The data owner only wants the users to access or modify parts of data files, and different users can access and modify different parts of the data. For example, the blogger can allow his friend to browse part of his private photos; enterprises can also authorize employees to access or modify part of sensitive data.

User: Cloud based services not only provide users with convenience, but also bring many security issues. Therefore, the study of access control scheme to protect users' privacy in cloud environment is of great significance.

We divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, we set read and write access permissions for users respectively. The Key-Aggregate Encryption (KAE) is exploited to implement the read access permission which improves the access efficiency. The users of PUD, a hierarchical attribute-based encryption (HABE) is applied to avoid the issues of single point of failure and complicated key distribution. Function and performance testing result shows that the PS-ACS scheme can achieve privacy protection in cloud based services.

The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security

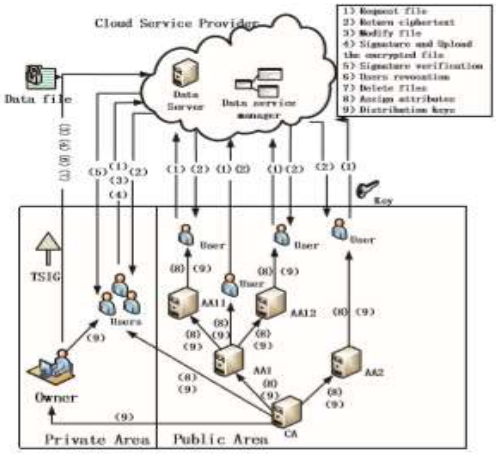
has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy.

Cloud:

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. 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.

The user can pass the cloud server's signature verification without disclosing the identity, and successfully modify the file.

SYSTEM ARCHITECTURE



SYSTEM DESIGN

UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

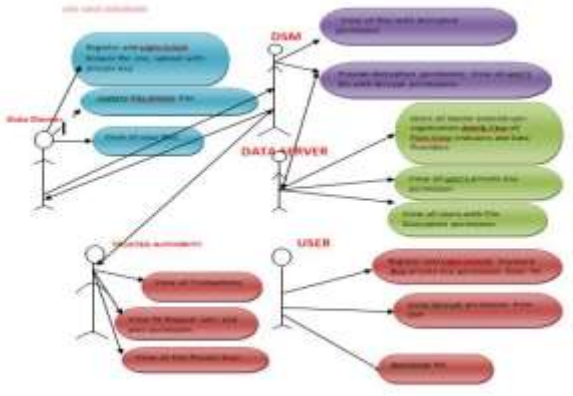
GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process. 4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

USE CASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



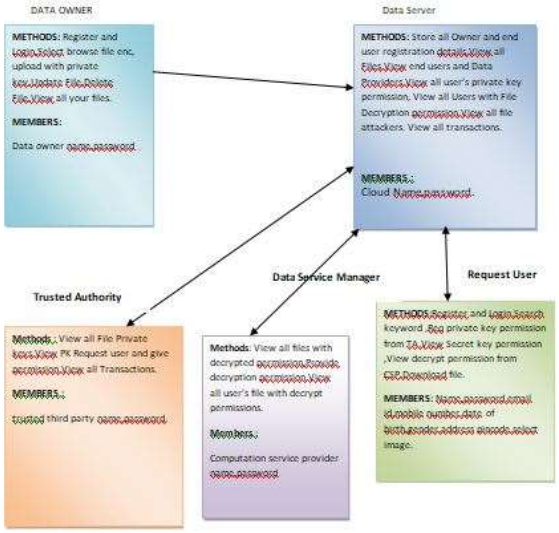
Journal of Engineering Sciences

Vol 11, Issue 7,July/2020

ISSN NO:0377-9254

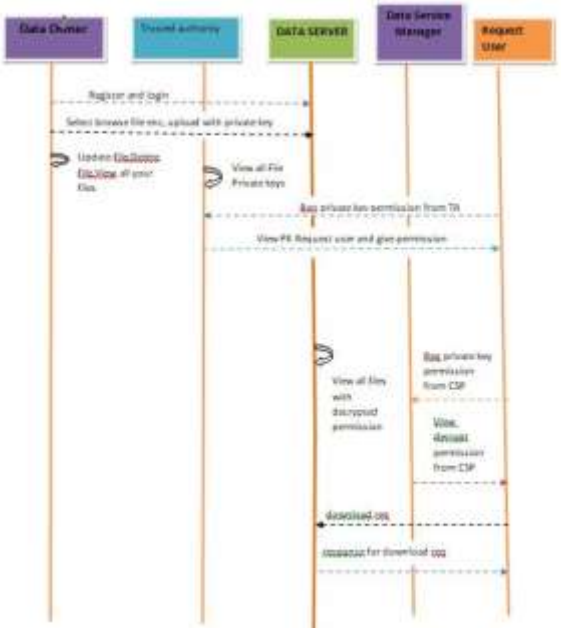
CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.



SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.



Client Server

IV.RESULTS:

Index.html

Data service manager login

Data service manager home page

Trusted authority login screen

Trusted authority home screen

Cloud login screen

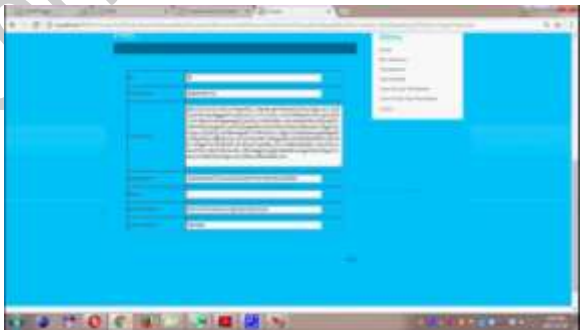
Cloud server home page

View end user details

Data provider details

View files

View file details



CONCLUSIONS

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.
[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.

AUTHORS PROFILES: Author 1:

Mr. B SEVA NAIK

GUIDE DETAILS:

Mr. B Seva Naik working as Assistant Professor in Mahaveer institute of science and technology affiliated to JNTUH as vast experience of 16 yrs in the teaching.

Completed his Master in software Engineering in JNTU College Engineering Anantapur Campus.

His area of interest subjects are Cloud Computing, Network Security, Data Based Security.

sevanaikb@gmail.com

Author 2:

Mr. ABDULLAH SHAREEF