ISSN 2250-3153

HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing

Sanchal Ramteke, Purva modi, Apurva Raghojiwar, Vijaya Karad, Prof.P.D. Kale

Computer, Pune University, India

Abstract- In several distributed systems using a certain set of attributes, a user should only be able to access data. Currently, the only method for enforcing such policies is to employ a trusted server to store the data. To keep the shared data confidential against any kind of misuse, a natural way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data. Previous Attribute - Based Encryption systems used attributes to describe the encrypted data. While in our system attributes are used to describe a user's credentials, and encrypting data determines a policy for who can decrypt. However, when organization users outsource confidential data for sharing on cloud servers, the adopted encryption system should not only support fine-grained access control, but also provide high performance, practicability, and scalability to best serve the needs of accessing data anytime and anywhere. This paper, proposes a scheme to help the organization to efficiently view and access confidential data on cloud servers. We achieve this goal by first combining the hierarchical identity-based encryption (HIBE) system and the CP-ABE system. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE.

Index Terms- Cloud computing, Flexibility, Scalability, Data Security

I. INTRODUCTION

With the emergence of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption system with a fine-grained access control to encrypt outsourced data [7].Cloud is a platform to store, retrieve, utilize multiple user's data .Benefits of using cloud computing involve reduced cost, easy and better operational facility, efficient database use and immediate response time. Though cloud is having multiple advantages, security in cloud is still a major issue. The contribution of paper involves creating a single cloud for multiple branches of the multiple countries providing hierarchy. User can easily store their data on the cloud and for providing security and privacy to this data stored on the cloud we are using encryption and decryption methods. We are implementing a system to achieve flexible and fine-grained access control of the users of the trusted cloud. The previous systems had proposed hierarchical attribute-based encryption (HABE) to achieve fine-grained access control in cloud storage services by combining hierarchical identity-based encryption (HIBE) and CP-ABE. In our paper, we are proposing hierarchical attribute set based encryption (HASBE) which is an extension to HABE .As our cloud computing model is service- oriented, we should take care of data from outsiders as well as from the cloud service provider itself. The scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in cloud computing. The security of proposed scheme is proved using the CP-ABE [1]. We are demonstrating the implementation of this paper for a software company. So, the service-oriented model used is Saas (Software as a Service). Hence the type of cloud we are using is private cloud.

II. LITERATURE REVIEW

In the existing system , multiple branches had an easy access to data of other branches. Also previously, the system was showing complete data related to the requested query even though the employee required some of the data. Due to this, the time to fetch and execute the query was too long. This increased the system response time thereby degrading the system performance. Another drawback was that the data was encrypted but the decryption was not restricted to that specific user as keys were not distributed in an efficient way resulting in retrieval of wrong data or incomplete requested data thus increasing chances of hacking. Incase if a lower level authority is absent or is on leave, work is completely stopped and is delayed for the leave duration. Previously, CP-ASBE policy was been used so the security of stored data was at risk and had chances of misuse as well. The drawback of this trend is that it is increasingly difficult to guarantee the security of data using traditional methods; when data is stored at several locations, the chances that one of them has been compromised increases dramatically. Organization users will face serious consequences if its data was disclosed. For these reasons the requirement is that the sensitive data is stored in an encrypted form so it will remain private and safe. Most existing public key encryption methods allow an organization to encrypt data to a particular user, but are unable to efficiently handle more expressive types of encrypted access control. Hence , less security was provided to the confidential data stored on cloud in previous system.

III. SYSTEM MODEL

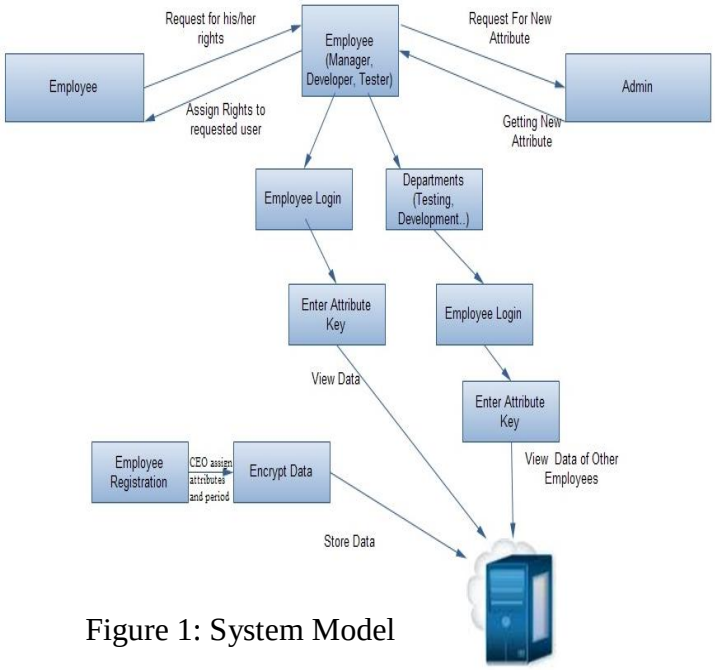


Figure 1: System Model

As mentioned in the above model Fig.1 we are concerned to implement following main responsibilities: Data Owner, Data Consumer, Domain Authority, Trusted Authority. User stores data on the cloud which can be retrieved by decrypting the same through a private key provided. This keeps the private data confidential. These users are monitored by the domain authority for their respective acceptance of correct key. In our case, the domain authority being the CEO alone, will handle total cloud environment. Top level authority can have access to lower level authorities . A Master-key is thus provided for higher level authorities to manage lower level authority's data. This requires storing of data in a secure manner so that it cannot be accessed by any outsider by illegal means. This system will allow the employee to view his personal information as well as carry tasks like request for leave or record updates if any using private domain securely.

Firstly, a user has to register with his entire attributes. Once user fills register form then the CEO approve all the details of user, after that CEO provide one key to user. When user gets that key he can access it like a password at the time of login. User will store all data by encryption public key and user can retrieve decrypted data which uses same public key and private key. After that, if user wants to see his own data then he uses the allotted private key and password. When manager wants to access employee's attribute then master key is used, which is generated by choosing the accessible attributes. If any lower authority is absent then higher authority is responsible for all work related to lower authority. When user is transferred from one location to another location, then all his data is updated in database itself. The manager will assign tasks and guide the employees working under him. Hence the management of assignment of tasks to employees should be done in a manner that is known to himself and respective employee with the permission of CEO in public domain. Also at the time of viewing of his personal information using private domain should be such that he could access it rather than some unauthorized user.

SET THEORY:

H is universal set i.e cloud.
H={E,B,U,R}
E=employee set
B=attribute set
U=user set
R=registered

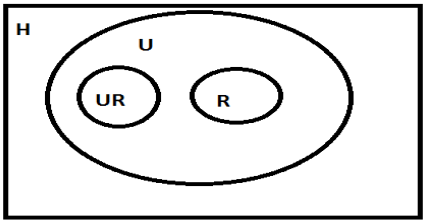
A] Identify the Employees
E= {e1, e2, e3….}
Where 'E' is main set of Employees like e1, e2, e3…

B] Identify the Attribute
B= {at1, at2, at3….}
Where 'B' is main set of registered Attribute like at1, at2, at3…

C] Identify the employee requested For Another Attribute
A= {raa1, raa2, raa3}
Where 'A' is main set of Request for another Attribute raa1, raa2, raa3

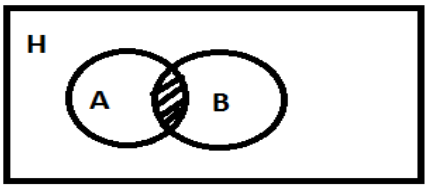
INITIAL STATE:

U={R, UR}
R=registered user
UR=unregistered user



INTERMEDIATE STATE:

Request for new attribute :
A=request for new attribute
B=contain all the attribute
R=provide requested attribute

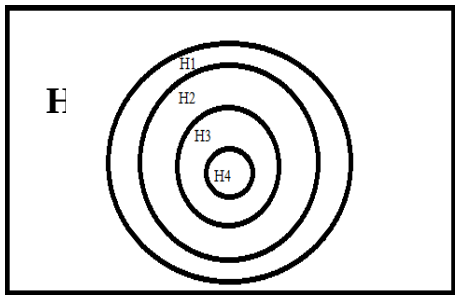


R = 

S1=A ∩ B

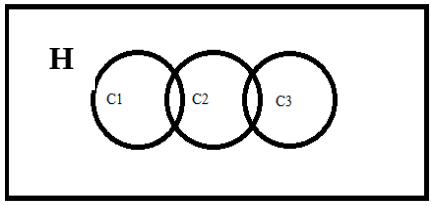
HIERARCHY:

H = {H1, H2, H3, H4}
where,
H is cloud
H1 is CEO.
H2 is general manager.
H3 is the list of managers.
H4 is the list of employees.



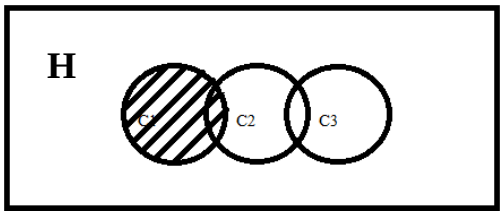
FLEXIBILITY:

H= {C1,C2,C3}
Where,
C1 is the old branch of the company where employee worked before transfer.
C2 is the employee being transferred.
C3 is the new branch where employee got transferred to.



H={C1,C2,C3}

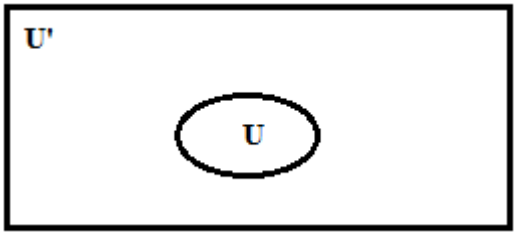
where,
s2 is employee data should be accessed to new branch only not old branch.



S2= (C1-C2) U C3

Scalability :

H = {H1,H2,H3,H4}
U={H1,H2}

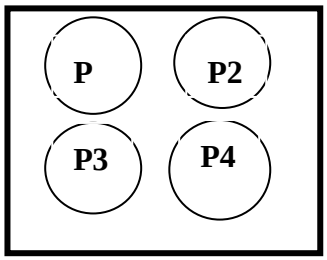


S3

U'={H3,H4}
U=present user
U'=absent user

FINAL STATE:

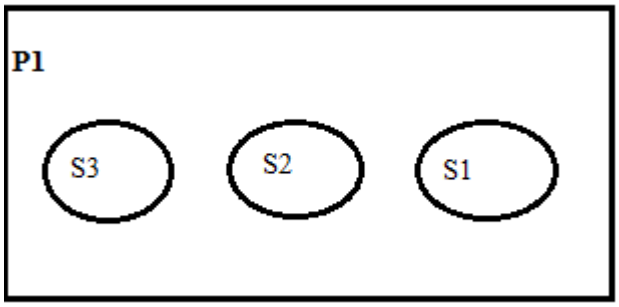
Identify the processes as P.
P= {Set of processes}
P = {P1, P2, P3,P4……}
Where
P1 ={S1,S2,S3}



Where :

{ S1= get new attribute after request}
{ S2= get new employee information when employee get transfer.}
{S3= get access of lower authority}.

Venn Diagram



IV. PROPOSED SYSTEM

In proposed system, instead of showing complete data, fetching of required data is carried out thus achieving fine-grained access control. This resulted in an efficient system response time as well as increased performance of the system. For security purpose, the proposed scheme consists of 3 keys: Private, Public and Master key. Public key is used in encryption of data, Private and public key is used to decrypt the data and

Master key is used for accessing the allowable data. We are also achieving scalability which manages the workload within company by assigning lower level authority task to higher level authority in case of lower level authority absence or leave. It also involves flexible access of data in which when an employee is transferred to another location/branch, the main database is updated. It reduces the work of manual data transfer. Another feature provided is User Revocation [5] that allows expiration of user's key to be updated after the duration of key is near to expiration. This system also maintains a single cloud with a main database for multiple branches as a virtual partition viewing as every branch has its own cloud.

V. CONCLUSION

Thus, we efficiently provide a fine grained access control with flexibility and scalability with a hierarchical structure in our HASBE system. Our contribution to this paper will be providing security to the users from outsiders or intruders by implementing session hijacking and session fixation security in our system. Also, a performance analysis will be done by the employee's updating monthly record performance.

APPENDIX

Sr no	**Term**	**Description**
1	**CP-ABE**	**Ciphertext-Policy Attribute-Based Encryption.**
2	**CP-ASBE**	**Ciphertext-Policy Attribute Set Based Encryption.**

REFERENCES

[1] Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption, Rakesh Bobba, Himanshu Khurana and Manoj Prabhakara University of Illinois at Urbana-ChampaignJuly 27, 2009.

[2] Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems Ayad F. Barsoum and M. Anwar Hasan Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada,2012.

[3] Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption, Suhair Alshehri, Stanisław Radziszowski, and Rajendra K. Raj Golisano College of Computing & Information Sciences ,Rochester Institute of Technology ,Rochester, New York 14623, USA2011.

[4] Gasbe: A Graded Attribute-Based Solution For Access Control In Cloud Computing, Chandana.V.R, Radhika Govankop,Rashmi N and R.Bharathi, International Conference on Advances in Computer and Electrical Engineering (ICACEE'2012) Nov. 17-18, 2012 Manila (Philippines) 2011.

[5] Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, Guojun Wanga,, Qin Liu a,b, Jie Wub, Minyi Guo c 2011.

[6] Cloud Computing Security Issues in Infrastructure as a Service, Pankaj Arora, Rubal Chaudhry Wadhawan Er. Satinder Pal Ahuja M.*Tech* CSE, *IGCE. Asstt.prof (CSE), IGCE Associate Professor & HOD (CSE),IGCE* Punjab technical Univ., 2012.

[7] Hierarchical Attribute-Based Encryption for Fine- Grained Access Control in Cloud Storage Services, Guojun Wang, Qin LiuSchool of Information Science and Engineering Central South University Changsha, Hunan Province, P. R. China, 410083,Jie Wu Dept. of Computer and Information Sciences Temple University Philadelphia, PA 19122, USA,2010.

AUTHOR

Correspondence Author- Sanchal Ramteke, sanchalr002 @gmail.com, m.purva19@gmail.com, no-7620996328.