

Implementation of HASBE Security technique in Cloud Computing

Rajesh Laxman Gaikwad., Prof. Dhananjay M Dakhane., Prof. Ravindra L Pardhi

*Dept of Computer Science and IT
Viva College of Arts Commerce and Science,
Virar, Maharashtra, India
rsv06@gmail.com*

Abstract-Cloud Computing is buzzword of modern era. We provide service to computing customers in form of SaaS (Software as a Service), IaaS (Infrastructure of Service), PaaS (Platform as a Service). These customers are ready to take service but the problem lies in security needed for their data place on cloud. The data in cloud should be safe. It is the cloud providers sole responsibility to provide security to the cloud. The Cloud providers heavily depend on Security Network technology. And Security depends on encryption techniques. Amongst several encryption technology such as ABE, ASBE, HABE and HASBE, HASBE is found to be more reliable and hence we shall use HASBE in our implementation of Security in Cloud Computing in this paper.

Keywords: Security; Encryption; access control; scalability; flexibility; fine grained.

1. INTRODUCTION

Cloud computing is a new paradigm that builds a virtualization, parallel and distributed computing, utility computing and service oriented architecture. Now days cloud computing is emerged service, that provides lot of benefits including the cost and capital expenditures, increased operational efficiencies, scalability and flexibility so on. Different cloud computing service providers provide the service oriented services such as Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a Service (SaaS). Based on this services IT industry will get fine state of infrastructure on the hardware/software and maintenances should be very easy. They save the cost on the Infrastructure and human resources.

Although the great benefits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security problems in cloud computing become serious obstacles which, without being appropriately addressed, will prevent cloud computing extensive applications and usage in the future. One of the prominent security concerns is data security and privacy in cloud computing is due to its Internet-based data storage and management.

The benefits of cloud computing will get lot of works from those work we considered a major problem is the security for the cloud data from users access limits and authorization service. The major constriction of our work will provide securable and with specific access control along with authentication and maintain the data security. To provide the data security there several works available, those works will be majorly on attribute based encryption and access control solutions. Here we are making an attempt to implement a network security model proposed as the Hierarchy Attribute Set Based Encryption (HASBE). It is expected that the HASBE network security model will prove highly scalable, flexible and fine grade in access control.

2. LITERATURE REVIEW AND RELATED

To provide the security and better access control we have several existing works available, those work will be major constrain on two process, those are **Attribute Based Encryption (ABE)** and **Access Control Solutions**.

Attribute Based Encryption

The Attribute Based Encryption method will propose by Sahai and Waters [1], a new method fuzzy identification based encryption. The draw backs of this scheme are lack of threshold semantics. The ABE scheme ciphertexts are not encrypted to one particular user as traditional public keys cryptography and user capable to decrypt the decryption key and cipher text key while matching the values. The ABE scheme will classified as the Key Policy Attribute Based Encryption (KP-ABE) and Cipher text Policy Attribute Based Encryption (CP-ABE).

KP-ABE [2], cipher texts is associated with a set of attributes and user's decryption key is associated with a monotonic tree access structure. Only if the attributes associated with the cipher texts satisfy the tree access structure, can the user decrypt the cipher texts.

CP-ABE scheme [3], the roles of cipher texts and decryption keys are switched, the cipher texts is encrypted with a tree access policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given cipher text, the key can be used to decrypt the cipher text.

Bobba et al [6] introduces cipher text policy attribute based encryption to organize the user attributes into a recursive set structure. The drawback of this approach it will hold the private key and not able to

combine the attributes sets.

Access Control Solutions

Yu et al [4] proposed access control scheme based on the KP-ABE, this approach is fine- gradient for the access control and scalable. In this approach use they specific symmetric data encryption key (DEK), this DEK will access generate a public key corresponding the KP- ABE, the key is generated according to structure of access. The files to upload the cloud with the encrypted format and data user will decrypt the file use DEK. The draw backs of this approach are encryptor will not able to decide who can decrypt the file.

Wang et al [5] proposed Hierarchical Attributed Based Encryption (HABE) to achieve the fine-grained access control in cloud storage by services combining HIBE and CP-ABE. The problem in this scheme is the same attribute may be administrated by multiple domain masters according to specific policies, which is difficult to implement in practice. Furthermore, compared with ASBE, this scheme cannot support compound attributes efficiently and does not support multiple values assignments.

3. ANALYSIS OF WORK

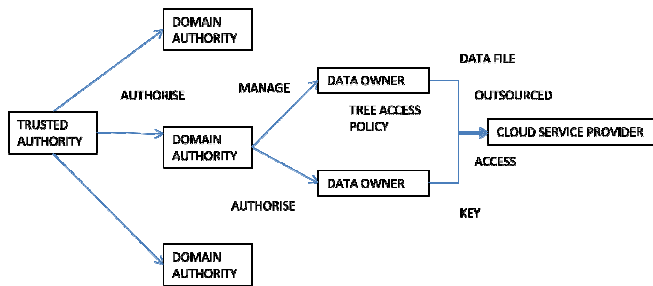


Figure 1: System Model

As shown in System Model Figure I, The computation complexity for each system operation in our scheme is as follows.

System Setup:

The System Setup calls the trusted authority, select the domain authority and generate the random number. To generate random number we apply several computational, the time complicity of system set up is $O(1)$.

Top – Level Domain Authority Grant:

This operation will do by trusted authority to generate the master key for the domain authority.
 $MK_i = (A, D, D_{ij}, D'_{ij}, \text{for all } a_{ij} \text{ belongs to } A, E_i \text{ for } A_i \text{ belongs to } A)$. The time complexity of the this process is $O(2N+M)$.

New User/Domain Authority Grant:

This operation will create a new user or domain authority along with the attribute sets. These operations do by the trusted authority. The time complexity of the process is $O(2N+M)$, where N is the number of

attributes in the set of the new user or domain authority, and M is the number of sets in A .

New File Creation:

this operation does by the data owner; to do this work we need the dek to encrypt the file. the time complexity of this process is $O(2|Y|+|X|)$ where Y denotes the leaf nodes and X denotes the translating nodes in tree access structure.

User Revocation:

This operation will do by the domain authority to maintain the user keys and encrypt the data files. The time complexity of this process is $O(1)$.

File Access:

This operation will do by the data consumer and this will test for the decryption algorithm process. The decryption process will impact on the scalability.

File Deletion:

This operation will do by the cloud provider based on the data owner's request. The time complexity of this process is $O(1)$.

4. SYSTEM ANALYSIS

computing is a new paradigm that builds a virtualization, parallel and distributed computing, utility computing and service oriented architecture. Now days cloud computing is emerged service, the cloud computing providing lot of benefits include the cost and capital expenditures, increased operational efficiencies, scalability and flexibility so on. Differ from the cloud computing provide the service oriented services such as Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a Service (SaaS). Based on this services IT industry will get fine state on the hardware/software maintenances should be very easy to state. They save the cost on the Infrastructure and human resources.

Although the great benefits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security problems in cloud computing become serious obstacles which, without being appropriately addressed, will prevent cloud computing extensive applications and usage in the future. One of the prominent security concerns is data security and privacy in cloud computing due to its Internet- based data storage and management.

The benefits of cloud computing will get lot of works from those work we considered a major problem is the security for the cloud data from users access limits and authorization service. The major constriction of our work will provide securable and with specific access control along with authentication and maintain the data security. To provide the data security there several works available,

those works will be majorly on attribute based encryption and access control solutions. Here we propose the Hierarchy Attribute Set Based Encryption (HASBE). The HASBE will prove high scalable, flexible and fine grade in access control.

A. Existing System

The major problem in the cloud computing is sharing the resources to all service requester either the requester should be same trusted authority or some other trusted authority, the second problem is providing data effectively when the service requested for the resources on the domain authority, third problem is providing security for the sensitive data from the third party vendors access limitations. To resolve these problems some existing schemes are available those details will observe on the following section.

B. Access control

Access control is security constrain based on this model several models available , the most effective two techniques are Bell-La Padila and BiBa, this techniques are flexible and fine grained access control. Some other approaches on access control are Principal of Policy in Secure group, Methods and limitations of security policy reconciliation etc. Unfortunately, these schemes are only applicable to systems in which data owners and the service providers are with in the same trusted domain.

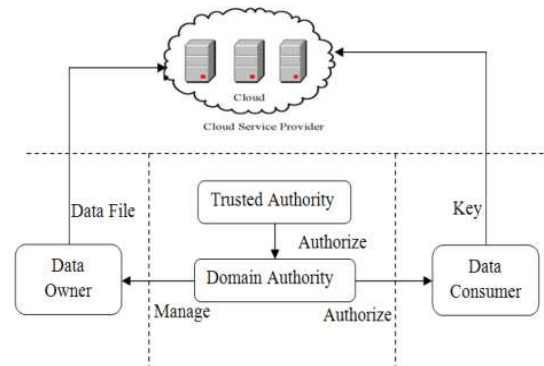
C. Attribute Based Encryption

Attribute based Encryption is technique to resolve the problem of the access control process, on this approach we have some existing systems those are Attribute based encryption for fine grained access control of encrypted data and Achieving secure, scalable, and fine grained data access control in cloud computing. This scheme falls short of flexibility in attribute management and lacks scalability in dealing with multiple-levels of attribute authorities.

D. Proposed System

To resolve the problems of existing work we propose a new approach is Hierarchy Attribute Set Based Encryption (HASBE), this approach is extension work for the Ciphertexts – Policy Attribute Set Based Encryption (CP-ASBE or ASBE). The propose work will solve the problems of access control and scalable. This work will majorly process access control system using the following parameters; they are cloud services provider, data owners, data consumers, domain authorities and trusted authority.

- The cloud service provider manages the cloud as the private data storage service.
- Data owners encrypt the files and store them in the cloud for



sharing with data consumers.

- Data consumers access the files and download the encrypted files and decrypt the files. The Data owner/consumer will administrated by the domain authority.
- The trusted authority is the root authority and responsible for manage the domain authorities.

5. SYSTEM ARCHITECTURE

E. System Modules

1. Trusted Authority
2. Domain Authority
3. Data Owner
4. Data Consumer
5. Cloud Service Provider

1. Trusted Authority

The Trusted Authority is responsible to system set up, top level domain authority grant; create domain authority and key update. The system set up process to create the public key and master key with considering the attribute sets range i.e depth, the hierarchy of domain services. The trusted authority create the domain with the unique id, before assign the unique to a domain it will check is valid domain or not if valid domain it will call the create domain authority function. The create domain authority function will give the unique id to create domain. Then the domain authority will able to create the sub domain and the users.

2. Domain Authority

The Domain Authority will able the create the new domain authority and new users, the domain authority created domains will be considering the sub domain authority, these domains authority will give the depth of the access tree structures, The each domain authority also able to create users, the user should a data owner or data consumer. To create the users it will having the functions

create user. The domain authority is also able to remove the users.

3. Data Owner

The data owner able to create file, encrypt file, re-encrypt file, file deletion permissions. The data owner to create a file, accept a unique id to the file and by using the encryption process encrypt the file and make tree structure access and store in the cloud. The data owner want to re encrypt file, it's possible with the accessing the file with the unique id and tree structure format. The data owner will also able to delete the file.

4 .Data Consumer

The data consumer will created by the domain authority, data consumer is able to access the cloud data by data owners provide, to access the data they need a key to access the file on the cloud, the key is provided by the domain authority. To get that key the data consumer needs to send the request to the domain authority, the domain authority checks the permissions then provide key. The key will contain the information of the file and decryption key value and access structure of the file. The data consumer will access the file by using the tree structure and unique id, and the data should read the file decrypt the file with the references of the decryption key.

5. Cloud Service Provider

- The cloud service provider manages a cloud to provide the data storage services.

6. SYSTEM DESIGN

Sequences and Collaboration Diagram for Data Owner

The figures 3 represent sequences and collaboration diagram for data owner. The data owner able to create file, encrypt file, re-encrypt file, file deletion permissions. The data owner to create a file, accept a unique id to the file and by using the encryption process encrypt the file and make tree structure access and store in the cloud. The data owner want to re encrypt file, it's possible with the accessing the file with the unique id and tree structure format. The data owner will also able to delete the file.

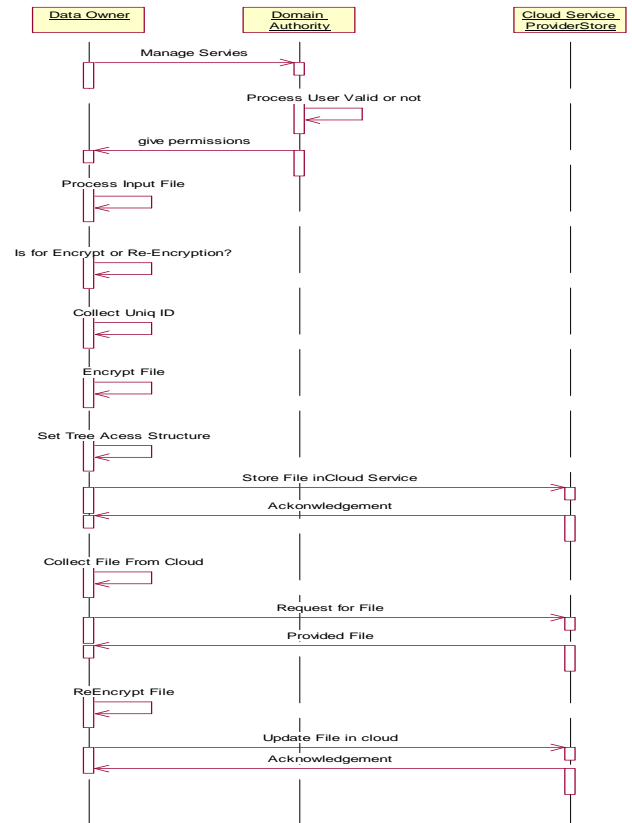


Figure 3 Sequence Diagram for Data Owner

4 Sequences and Collaboration Diagram for Data Consumer

The figures 4 represent sequences and collaboration diagram for data consumer. The data consumer will created by the domain authority, data consumer is able to access the cloud data by data owners provide, to access the data they need a key to access the file on the cloud, the key is provided by the domain authority. To get that key the data consumer needs to send the request to the domain authority, the domain authority checks the permissions then provide key. The key will contain the information of the file and decryption key value and access structure of the file. The data consumer will access the file by using the tree structure and unique id, and the data should read the file decrypt the file with the references of the decryption key.

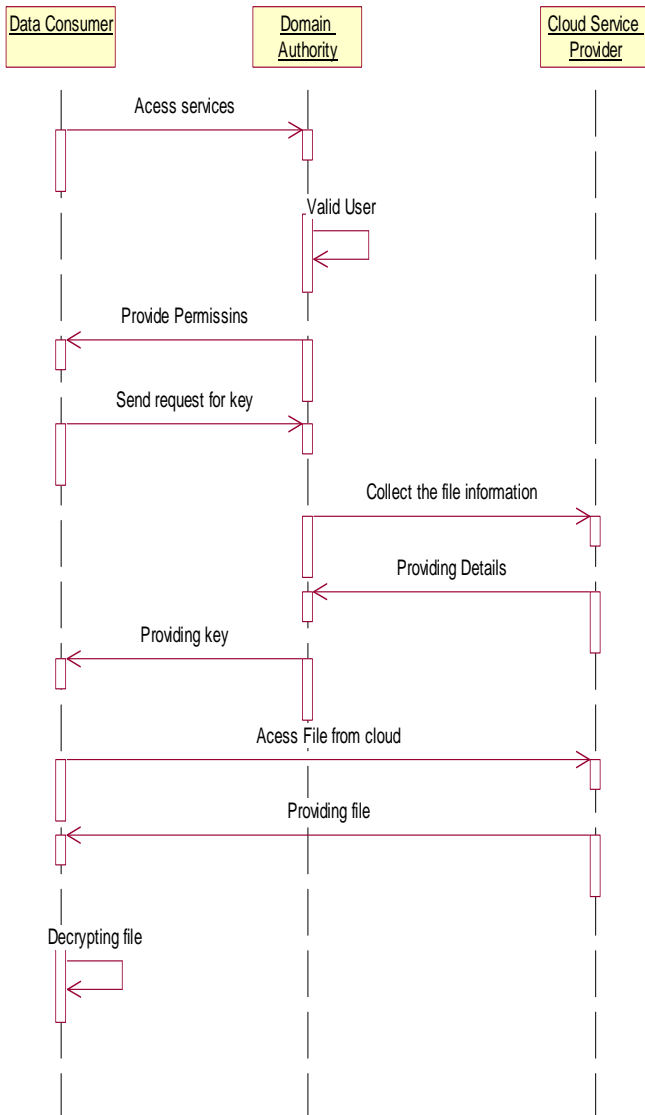


Figure 4 Sequences Diagram for Data Consumer

Hardware and Software Requirements

Hardware Specifications

The hardware used for the development of the project is:

Processor	: Pentium IV
Ram	: 1 GB
Hard Disk	: 80GB

Software Specifications

The software used for the development of the project is:

Operating Systems	: Windows XP/2007
Environment	

Web Server	: Tomcat
Languages	: JAVA, JSP, Servlets, java-cryptography API
Database	: MS-SQL Server 2000




7. ACKNOWLEDGMENT

This paper is attempt to implement HASBE Technique of encryption and suggestion are well-come. I owe my thanks to eminent gurus of encryption Prof. Dhananjay Dakhane, Prof Ravindra Pardhi , Prof Prashant Jena, Prof Dhamesh Rathod, Prof. Minesh Ade who guided through this paper.

8. REFERENCES

- [1]. Sahai and B. Waters, "Fuzzy identity based encryption," in *Proc. Advances in Cryptology—Eurocrypt*, 2005, vol. 3494, LNCS, pp. 457–473.
- [2]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Alexandria, VA, 2006.
- [3]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, 2007.
- [4]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM 2010*, 2010, pp. 534–542.
- [5]. G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Chicago, IL, 2010.
- [6]. R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in *Proc. ESORICS*, Saint Malo, France, 2009.
- [7]. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing Zhiguo Wan, Jun'e Liu, and Robert H. Deng, *Senior Member, IEEE*.

AUTHORS

	<p>Prof. Rajesh L Gaikwad, Currently working as a lecturer in Viva College and pursuing M.E. (Computer Engg) from Sipna COE&T, Amravati which is affiliated to SGB Amravati University. The Area of Interest is Network Security.</p>		<p>Prof. Ravindra L. Pardhi has done M.E. (Information Technology). He is an Assistant Professor with 5 Years of experience in Sipna COE&T, Amravati which is affiliated to SGB Amravati University. His area of interest is Web Technology ,Object Oriented Programming.</p>
	<p>Prof. Dhananjay M. Dakhane has done M.E in Computer Engg. and pursuing Ph. D. He is an Associate Professor with 14 years of experience in Sipna COE&T, Amravati which is affiliated to SGB Amravati University. The Area of Interest is Network Administration and Security, Operating Systems.</p>		