Privacy-Aware Access Control System in UCSH Private Cloud Using Identity-based Encryption (IBE) and Signature (IBS)

Ei Ei Mon
University of Computer Studies, Hinthada
eemucsy@gmail.com

Win Win Thant
University of Computer Studies, Hinthada
winwinthant@gmail.com

Abstract: *Privacy protection plays a vital role to build up the cloud computing environment. Especially the cloud data storages and data centers must provide and protect individual cloud user's privacy according to predefined service level agreement (SLA) policies. This system intends to implement secure privacy-aware access control system using Identity based Encryption (IBE) and Identity based Signature (IBS) algorithms, that do not have to generate the keys itself in UCSH Private Cloud. IBE and IBS systems allow any party such as cloud provider, cloud user and trusted third party to generate a public key from a known unique identity value. The corresponding private keys are generated by Private Key Generator (PKG). The proposed system generates public key and private key of cloud service provider (CSP) and cloud users by PKG using IBE and IBS for each user group. When data sent from server to client, first data is encrypted using secret key algorithm. Then key is encrypted using public key of user. Data is signed using the private key of server for the authentication of sender. This system will be implemented as cloud server and cloud client where cloud server stores client data in its data center. Java programming will be used to implement the system. The proposed system provides the private cloud to enhance privacy and security of data.*

Keywords: privacy; identity based encryption; identity based signature; private key generator

1. INTRODUCTION

Cloud computing is a style of computing in which dynamically scalable and visualized resources are provided as a service over the internet. Consumers and businesses are willing to use online computing only if they trust that their data will remain private and secure. The ability of cloud computing providers is not only cloud services but also for protecting the fundamental rights of privacy. This paper presents policies and practices for addressing privacy issues and enabling greater trust in the cloud service providers. Identity- based Encryption and Signature is used in the process of privacy control.

Traditional public key cryptosystems use very long integers, typically 2048 bits, as public keys. These systems rely on digital certificates to connect an identity like a person or a machine to a public key. Identity-based systems have the advantage that a public key is the identity, usually an arbitrary string like an email address. As a result, identity-based cryptography significantly reduces the system complexity and the cost of establishing and managing the public key authentication framework. In this system, there is one root PKG is set up to generate the public keys for the cloud server and clients. To encrypt a message to cloud client CC1, cloud provider only needs to obtain the public parameters of CC1's root PKG and his identity. It is especially useful in large companies or e-government structure where there are hierarchical administrative issues needed to be taken care.

The paper is organized as the following: Section 1 is the introduction, section 2 is related works. In addition, section 3 is background theory; section 4 represents the proposed system, and section 5 represents implementation of the proposed system. Section 6 is the conclusion of the system, Section 7 is the acknowledgements and Section 8 represents the references.

2. RELATED WORKS

In a traditional symmetric key cryptosystem (SKC), a shared key between a sender and all recipients is used as an encryption key and a decryption key. When a sender wants to encrynpt a file to n recipients, he first chooses a unique shared key corresponding to the file and sends it to all recipients in a secure way, and then encrypts the file using the shared key. Finally, the corresponding ciphertext is stored in a cloud. Therefore, the key size will grow linearly with the number of ciphertexts.

As Neuman et al. have noted [1] the traditional Kerberos presents an attractive security target in the form of the KDC which maintains a shared symmetric key with every principal in the realm. In the event of a KDC compromise, all the symmetric keys will be divulged to the attacker and will have to be revoked. Recovering from such a compromise requires the re- establishment of new shared keys with all principals in the realm. Such a recovery is very costly in terms of time, effort and financial resources.

In [4], A threshold-based model for privacy protection in cloud computing is presented by Ren, Chen, Zhang and Ma. In this paper, a special secret sharing scheme based on (n +1, t +1) threshold is proposed. This scheme assigns each row of the matrix to participant as a sub-key and makes use of the linear correlation and linear independence of the vectors to evaluate the rank of the key matrix. Nobody including the cloud service providers can

recover the data without the permission of the data owner. This scheme greatly enhanced the security of user's data. But it does not contain the authority research on the basis.

[7] introduced outsourcing computation into IBE and propose a revocable conspire which are designated to CSP. It accomplishes steady effectiveness for both calculation at PKG and private key size at client. User needs not to contact with PKG amid key-refresh, PKG is permitted to be disconnected subsequent to sending the disavowal rundown to KU-CSP and no protected channel or client validation is required a mid key-refresh amongst client and KU-CSP.

3. THEORYBACKGROUND

Privacy is the fundamental human right, also named as "the right to be left alone" and "control of information about ourselves". Taxonomy of privacy has been produced that focuses on the harms that arise from privacy violations, and this can provide a helpful basic on which to develop a risk / benefit analysis.

Key aspects of cloud computing are that there is an infrastructure shared between organizations that is off premise. Therefore, there are threats associated with the fact that the data is stored and processed remotely, and because there is an increased usage of virtualized and sharing of platforms between users. Protection of personal, confidential and sensitive data stored in the cloud is therefore extremely important. Moreover, personal and sensitive data may move around within an organization and / or across organizational boundaries, so adequate protection of this information and legal compliance must be maintained despite the changes. The main primary risks of cloud computing are–

- For the cloud user: being forced or persuaded to be tracked or give personal information against their will, or in a way in which they feel uncomfortable.
- For the organization using the cloud service: non-compliance to enterprise policies and legislation, loss of reputation and credibility.
- For implementers of cloud platforms: exposure of sensitive information stored on the platforms (potentially for fraudulent purposes), legal reliability, loss of reputation and credibility, lack of user trust and take-up.
- For providers of applications on top of cloud platforms: legal non-compliance, loss of reputation, 'function creep' using the personal information stored on the cloud, i.e., it might later be used for purposes other than the original cloud service intension.
- For the data subject: exposure of personal information.[6]

4. THE PROPOSED SYSTEM

This system presents the privacy control over cloud computing where cloud server provides data service for academic record information. Identity based Encryption method is used to protect the data from threats.

According to Figure 1, there are three main components in the proposed system: Cloud Service Provider (Cloud Server), Cloud User (Cloud Client) and Trusted Third Party (PKG). Providers of Cloud-based services usually maintain different distributed data storages. This allows to dynamically adapting the resources provided for a particular customer based on their current needs. Databases in the cloud computing system are either directly visible or accessible to customers as part of the infrastructure/platform, or are hidden behind service interfaces. This system will be mainly based on data secrecy, privacy and confidentiality of private cloud computing environment. Identity based cryptography is used to control secrecy, privacy and confidentiality of data when accessed by each cloud user.

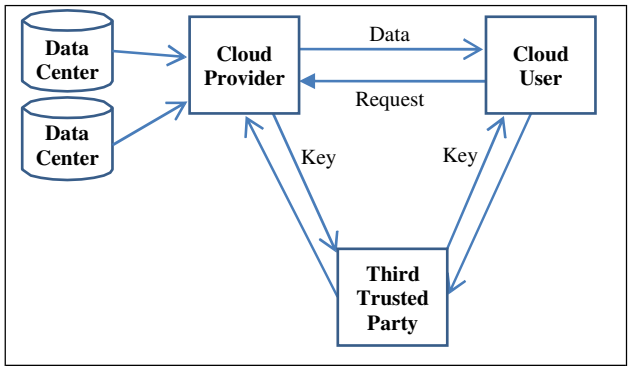

Figure 1. System design of the proposed system

4.1. Identity-based Encryption

In 1984, Shamir [3] proposed a concept of identity- based cryptography. In this new paradigm of cryptography, users' identifier information such as email or IP addresses instead of digital certificates can be used as public key for encryption or signature verification. As a result, identity-based cryptography significantly reduces the system complexity and the cost for establishing and managing the public key authentication framework known as Public Key Infrastructure (PKI).

Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could include an email address, domain name, or a physical IP address. Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the private key generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which

uses the master private key to generate the private key for identity ID.

4.2. System Design

This system presents identity based authentication for cloud computing. Cloud service provider provides cloud storage as a service to the cloud clients. Data Storage in this system includes shared data storage as well as individual data storage as in Figure 2.

There is one root PKG (TTP) that is generating public key based on user's identity and private key. In the middle level, there are group main nodes (for departments). Cloud clients are child nodes of each group. Each cloud client in the cloud computing has a unique name. The name is the client's registered name (User ID) when the client joins the cloud storage service. The identity of the node is defined as the string from root node as user ID + group name.

The process design of the system is shown in Figure 2. Cloud client sends access request along with its ID to CSP. CSP gets the public key of client (PK Client) from PKG server using ID of client. Requested data is encrypted by Secret key algorithm AES. Then secret key is encrypted using PK Client. Then it is signed by private key of server (SK Server) for the authentication process to make sure server is the right sender to the client. Encrypted data and signature are sent back to the client. In the client side, client gets the public key of server (PK Client) from the ID of server. First requested data is verified using PK Server. After the verification process, first key decryption is performed to get the secret key of AES algorithm using private key of client (SK Client) to make sure client is the right person to receive the data. Then encrypted data is decrypted by AES algorithm. In this system Data Encryption will be performed by symmetric algorithm, also known as secret key algorithm, AES and asymmetric algorithm, a public key algorithm, RSA will be used in key encryption. In signing the document, digital signature (Secured Hash Algorithm – SHA) will be used.

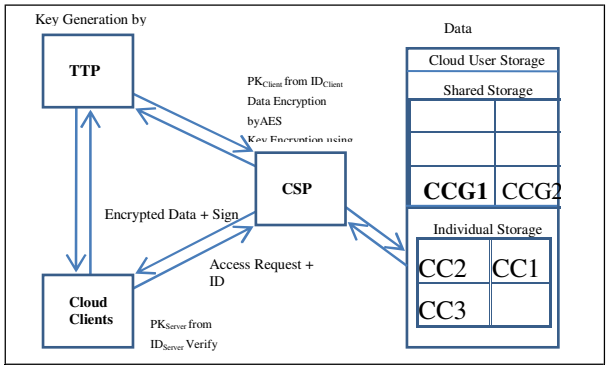

Figure 2. System Design

PK = public key, SK = private key

4.3. Types of Users and Groups

Private cloud users of the Proposed System are as follows:

- school administrators,
- teachers,
- staff and
- students

Groups are categorized based on their roles as follows:

- Department of the teachers, admin department for school administrators and student affair department for thestaff.
- For students, groups will be just 'Student' group.

4.4. Functions of CSP

In this system, cloud service provider provides cloud storage and privacy and security control over the cloud storage. Data storage for academic records of students and private data for each student will be provided. Cloud users can be school administrators, teachers, staff and students. Groups are categorized based on the department of the teachers, admin department for school administrators and student affair department for the staff.

4.4.1. Identifying Registered Users and Users Groups

When cloud user requests data from storage of cloud service provider, requested user and user's group must be identified first. In the authentication process, user provides its ID including its group along with its password. ID and group are checked against CSP's registered list. If authentication information of user is valid, user is allowed to access the data based on service policy.

4.4.2. Available Services on Cloud Service Provider

Cloud service provider, in this system, delivers storage as service. It includes shared data storage as well as individual data storage. Access to shared data service is performed by the access policy defined by organization. Access policy includes roles and permissions based on the group of user and user role in the organization. Permissions are READ / WRITE permissions on data objects. Those permissions are assigned to roles and roles are assigned to users. Access to shared data is controlled by the permissions of roles assigned to user.

Students can access only individual data storage, where students can create their own data and access to it. Individual data cannot be shared. It's READ / WRITE access is only permitted to its owner.

Upon receiving the storage request (READ Access), CSP performs following operation

- Identifying User and User Group
- Get Requested Data from data storage
- Get cloud user's public key from PKG using ID of cloud user (ID = user ID + group name, user ID are unique)
- Get provider's private key from PKG

- Data is encrypted using public key of cloud user.
- Then encrypted data is signed using the private key of provider
- Encrypted data and signature are then sent to cloud user.

4.4.3. Service Level Agreement (SLA)

Service Level agreement is a contract between cloud provider and cloud user that specifies the level of service expected during its term. Service based SLA is an agreement for all cloud users using the services being delivered by the service provider. Following agreements are the SLA for CSP in the privacy point of view.

- Access of shared storage is controlled by access policy of the organization.
- Individual storage cannot be shared between cloud users.
- Students can post their own data on individual storage and students do not have right to access shared data.

4.4.4. Access Control Policy

Cloud service provider, in this system, delivers storage as service. It includes shared data storage as well as individual data storage.

- Individual data storage (shared data service) is only for Student users, where READ / WRITE access is only permitted to its owner.
- Access to shared data service is performed by the access policy defined by organization. It is controlled by the permissions of roles assigned to user.

The following table shows example of permission assignment to each role.

Table 1. Example access permissions on data objects

	Student	**Mark**	**Exam**	**Subject**	**Teacher**	**Staff**
Rector	R + W	R	R + W	R	R	R
Professor	R + W	R + W	R + W	R + W	R + W	R
Lecturer	R + W	R + W	R	R	R	R
Tutor	R	-	R	R	R	R
Staff	R	-	R	R	-	-
Student	R(Own)	R(Own)	R	R	-	-

4.5. Functions of Cloud Client

Cloud users can be school administrators, teachers, staff and students. Cloud user sends access request of required data to the cloud provider along with its ID.

- Identifying
- Checking SLA
- Generate Keys through TTP

Upon receiving the requested data from cloud service provider, cloud client performs the following process:

- Get Encrypted data and signature from cloud service provider
- Get provider's public key from PKG
- Get cloud user's private key
- Signature is verified using the public key of provider to make sure data is not modified and authentication of sender
- If the signature is verified, encrypted data is decrypted using private key of cloud user.

4.6. Key Generation by IBE and IBS

In this system, PKG is trusted third party, which is responsible for key generation process. This system uses IBE approach where unique identity of user is used public key computation. PKG has the following process:

Let X be the input user and IDX = ID of user X
Randomly choose two large primes P, Q, where P ≠ Q.
□ = P-1 * Q-1 N = P * Q
B = Hash(IDX)
E = BigInteger (B);
Compute D, such that D * E = 1, ED = 1 mod □
Public-Key = {N, E} Private-Key = {N, D}

In the following example, instead of generating large integers, we will use small integer. For user eem:
Let P = 17, Q = 11
□ = P-1 * Q-1 = 17 – 1 * 11 – 1 =
160 N = P * Q = 187
Let H(eem) = 7 = 111.
E = 7
Compute D □D * E = 1 mod □ and D <□
D = 23
Private key = {N, D} = {187, 23} Public key = {N, E} = {187, 7}

4.7. Implementation Process

The process flow of the CSP and CC over sending and receiving is shown in Figure 3 and Figure 4. In this section, the algorithms of the proposed system are represented as follows:

Algorithm: *EncryptByIBE*
Input: receiver id as RID, Data data
Output: Cipher cipher
Begin

```
PublicKeypkey = PKG.RequestPublicKey(RID);
if (pkey == null) Error ("Invalid Receiver");
Cipher cipher = IBE.Encrypt (data, pkey);
return cipher;
```

End

Algorithm: *DecryptByIBE*
Input: Receiver id as RID, Cipher cipher
Output: Data data
Begin
PrivateKeypkey = PKG.RequestPrivateKey(RID, password);
if (pkey == null) Error ("Receiver Authentication Failed!");
Data data = RSA.Decrypt (cipher, pkey);
return data;
End

Algorithm: SignedByIBS
Input: sender id as SID, Data data
Output: Signature sign
Begin
PrivateKeypkey = PKG.RequestPrivateKey(RID, password);
if (pkey == null)
Error ("Authetication Failed!");
Signature sign = DigitalSignature.Sign(Data, pkey)
return sign;
End

Algorithm: SignedByIBS
Input: Signature sign, SenderID as SID
Output: Message
Begin
PublicKeypkey=PKG.RequestPublicKey(SID, password);
if (pkey == null)
Error ("Invalid Sender!");
booleanbverify =DigitalSignature.Verify(sign, pkey)
if (bverify) Message = "Signature Verified";
else Message = "Not Verified";
End

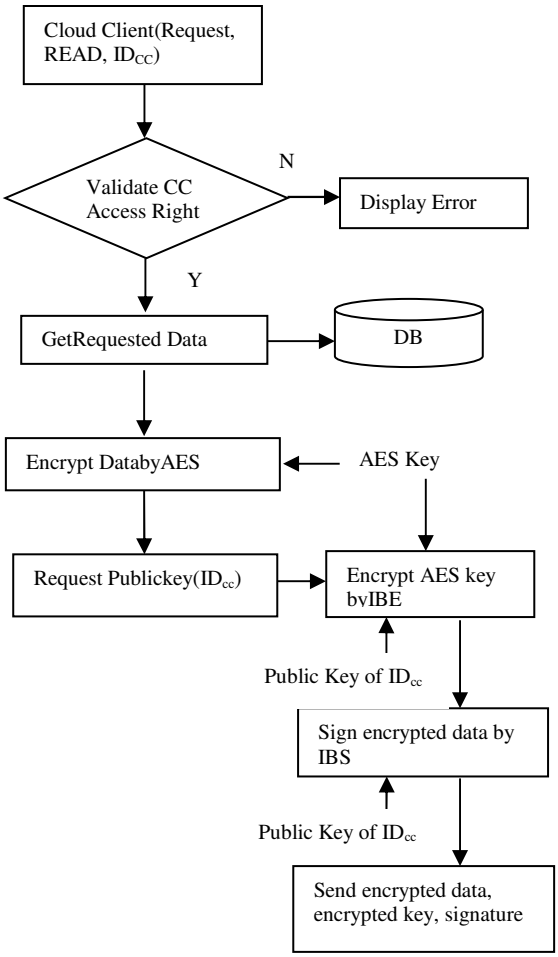

Figure 3. Process flow of CSP for data sending

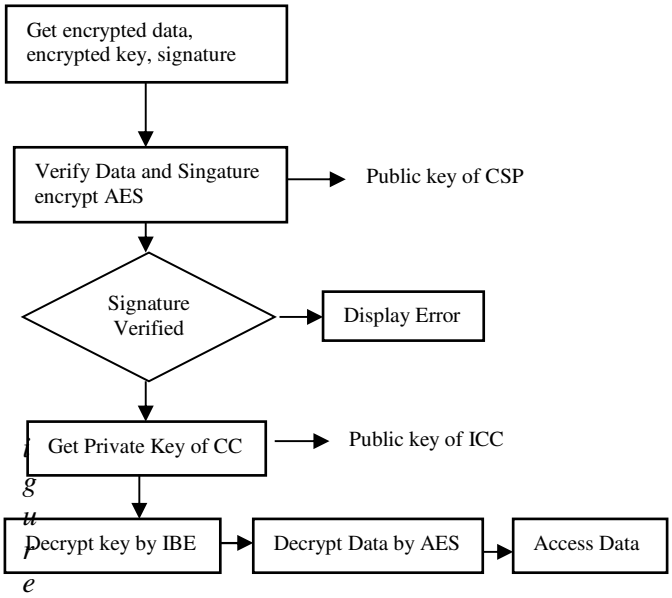

Figure 4:

Figure 4: Process flow of CC for data receiving

Roles and access permissions defined in this system are as follows:

- Roles can be created for the various job functions in an organization and users then assigned roles

based on their responsibilities and qualifications.

File Size	AES (E)	AES (D)	IBE (E)	IBE (D)
22 KB	638	21	168	21
998 KB	328	33	3864	33
768 KB	220	32	2387	32
89 KB	932	10	748	10
123 KB	221	28	1076	28

- Users can be easily reassigned from one role to another.
- Roles can be granted new permissions, and permissions can be revoked from roles as needed.
- In this system, permissions to access the objects are assigned based on the role of the user.
- For example, there are two permissions 'READ' and 'WRITE' for the object STUDENT.
- Lecturer has 'READ' and 'WRITE' permissions while Staff Role has 'WRITE' permission to STUDENT object.
- Access to STUDENT object is controlled based on the role of the requested user.

5. SYSTEM IMPLEMENTATION

This system is implemented using Java programming language. There are three components implemented in this system, Cloud Service Provider (CSP), Cloud Client (CC) and Trusted Third Party (TTP) for key generation. Remote Method Invocation (RMI) protocol is used to communicate between each component. Implementation of those components is as follows:

- CSP (Cloud Service Provider) –includes cloud simulation which invokes Cloud VM for the cloud user. Privacy functions and policies are also installed in the CSP.
- TTP (Trusted Third Party) – responsible for generating keys for IBE and IBS.
- CC (Cloud Client) – cloud user of CSP, include front end tools to access data from CSP. Access is controlled by role of cloud user and privacy setting between cloud users.
- Implementation of Cloud Simulation Scenario is as follows:
- Cloud VM is launched for each and every cloud user
- It is responsible for performing tasks of each user.
- In general, the functions of VMWare can offer unified computing and storage resources.

5.1. Experimental Results

In this system, different files with different file sizes are tested with both IBE and AES. Processing time in milli-seconds for those algorithms is shown in Table3. According to the experimental results, the processing time is not different AES and IBE in decryption but it is less time for encryption with IBE for smaller file size and more secure than AES and enhance privacy of data.

Table 2. Processing times for AES and IBE

6. CONCLUSIONS

The proposed system presents the privacy control over cloud computing environment. To prepare for the growth of cloud computing, the proposed system will implement clear and transparent data handling processes with a set of flexible management tools in its enterprise platform offerings that help to protect sensitive and confidential data. It will provide security policy within the cloud computing server, while traveling over internet and authentication of user at the client side. In the proposed system, privacy of cloud data service is controlled by the identity-based encryption and signature. Even though the use of identity based cryptology is limited to the environment where the PKG is unconditionally trusted, in non-identity-based-cryptography, the revocation of the public key is a big problem in that users who want to encrypt messages or verify signatures should first check whether the concerning public keys have been revoked or not. The proposed system provides the private cloud to enhance privacy and security of data.

7. ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their insightful comments on this paper.

8. REFERENCES

B.C. Neuman, B. Tung, J. Wray and J. Trostle, "Public Key Cryptography for Initial Authentication in Kerberos", Internet Draft, October 1996. (ftp://ietf.org/internetdrafts/draft-ietf-cat-kerberos-pk- init-02.txt).

S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", HP Labs, Bristol, UK, 2009.

A. Shamir, "Identity-based Cryptosystems and Signature Schemes", Proceedings of CRYPTO '84, LNCS 196, Springer-Verlag, 1984, pp-47-53.

X. Ren, L. Chen, J. Zhang and X. Ma, "A Threshold-based Model for Privacy Protection in Cloud Computing", Advances in Information Sciences and Service Sciences. Volume 3, Number 3, April2011.

G. Wang, Q. Liu, and J. Wu, "Achieving Fine-grained Access Control for Secure Data Sharing on Cloud Servers", CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE Concurrency Computat.:Pract. Exper.2000.

S. Srinivasamurthy, D. Q. Liu, A. V. Vasilakos, N. Xiong, "Security and Privacy in Cloud Computing: ASurvey", PCC Vol. 2 Iss. 4, 2013, pp.126-149.

C. Mukundha, "Identity Based Encryption in Cloud Computing With Outsourced Revocation Using Ku-Csp."IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 8, 2018, pp. 12-21.