AMELIORATE SECURITY POLICY USING MEDIATED RSA AND IDENTITY BASED CRYPTOGRAPHY IN CLOUD COMPUTING

[1] RAVI J. KHIMANI, [2] NISHANT S. SANGHANI, [3] ASST. PROF. K.K. SUTARIA

[1, 2] Computer Engineering Department, V.V.P. Engineering College, Rajkot, Gujarat, India

[3]Asst. Professor, Computer Engineering Department, V.V.P. Engineering College, Rajkot, Gujarat, India

khimani.ravi@gmail.com, nishantssn@yahoo.co.in, kamal.sutaria@gmail.com

***ABSTRACT*:** *Cloud computing is becoming very important framework to provide number of services like, data storage, computation, infrastructure, software etc .over internet through virtualization of systems. So, security of data in all those services needs to consider. Attacker can try to attack on data or communication and can harm the system. Such attacks are like man-in-the-middle attack, chosen plaintext, chosen ciphertext, denial of services. There are techniques exist like Public key Infrastructure (PKI) to prevent attacks. In this paper, a proposed system is discussed which can be used to prevent data from such attacks. This proposed technique is combination of Identity Based Encryption (IBE) and Mediated RSA (mRSA) techniques for Cloud environment. The IBE is used to reduce difficulties and overhead of certificate management during communication between users. It is done by using Hash functions. And Mediated RSA technique is used to provide easy key generation and key management during communication and to remove some critical problems exist in PKI.*

KEYWORDS: Identity Based Encryption, Mediated RSA, Cloud Computing, IBE in Cloud, Key Escrow.

1. INTRODUCTION

Cloud Computing is technology considered as next generation architecture of IT Organizations. In computation field, there are number of ways for providing distribution and parallelism of resources to improve performance and utilize available resources. Cloud computing is a platform for data storage, processing and delivery in which available resources are given virtually to the clients as per demand [1].

Cloud Computing is a model which provide computation services, network access to the pool of shared computing resources on demand with minimal management effort and without Service Provider interaction [2].

Cloud computing provides services to user without knowledge of physical location and configuration of the systems that deliver these services. This takes form of Web based tools that clients can access through Internet. These applications and data are stored at remote location. The computing and storage resources are unified at remote data centre location [3].

Cloud Computing has five essential characteristics as follows,[3]

On Demand Self-Service

A user can access computational resources, networks and data storage equipments as per need and on demand without making interaction with service provider.

Broad Network Access

The information and resources can be accessed from anywhere and anytime and from any heterogeneous platforms and devices.

Resource Pooling

All the computational resources, network resources and data storage resources are provided to the user from a large pool of resources and different users can access same pool without knowledge of location.

Rapid Elasticity

Resources are provided to users quickly and easier. This can be done by assigning resources when required and released when no longer needed.

Measured Services

Users use the resources as their need and pay only for those services and resources. So, those can be automatically optimized and controlled.

Cloud Computing provides three types of services that are, [4]

Software-as-a-Services (SaaS)

It provides the use of applications running on the Cloud Provider's infrastructure. These services can be accessible from any heterogeneous systems or any interfaces. These services may be defined with exception of limited user specific usage.

Product-as-a-Service (PaaS)

It provides development platform to the user to develop applications using the tools provided by the PaaS provider and they already know how to use

those tools. Then they deploy application to the PaaS provider Cloud. It provides core cloud competences those are required to develop applications onto the Cloud.

Infrastructure-as-a-Serivece (IaaS)

It provides provision of network, processing and other resources where user can deploy and run the applications. User has not any control on infrastructure of Cloud but can control deployed application. IaaS can deliver software, data centre space, virtualization platforms and network instruments with advantages like flexibility, scalability and cost effectiveness.

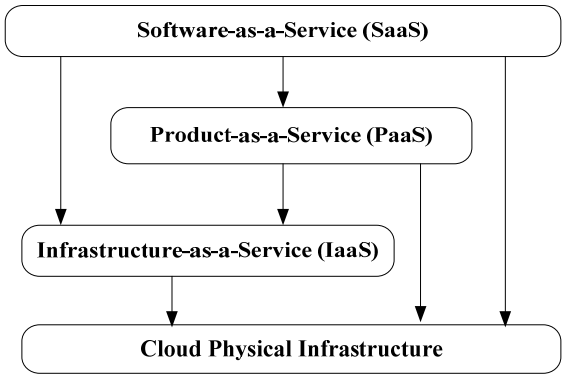

Fig.1 Services provided by Cloud Computing

Cloud Computing technology and services can be deployed in number of ways according to their purpose and characteristics. This deployment of Cloud is categorized in four ways as follows [3].

Private Cloud

In this Model of Cloud, Infrastructure is deployed and operated by an Organization privately where all the resources can be owned, maintained and controlled by it only. It may be managed or hosted by Third-party also.

Community Cloud

In this Cloud, Infrastructure of Cloud is deployed on shared web space and operated by several organizations in sharing that supports a specific community with common approaches, demands and usage.

Public Cloud

In this Cloud, Infrastructure of Cloud is available to the general public or large group of different kinds of organizations. Client can access services without and any control and at specific rent. Client's services and data can be co-located with other users.

Hybrid Cloud

In this Cloud, Infrastructure of Cloud can be combination of Public, Private and Community Cloud Infrastructure. This combination of two or more clouds is with unique characteristics, entities and benefits to the users. So, programs and data can be transferred from one system to another system.

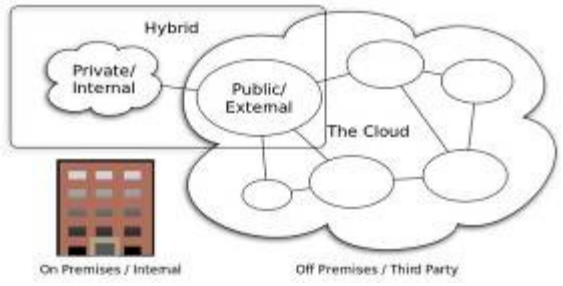

Fig.2 Deployment Models of Cloud

2. IDENTITY BASED ENCRYPTION

As Cloud is used to store large number of data and to transfer data, security is main concern to those data. Intruder can attack to ongoing communication or storage devices and harm system in different ways. There are number of attacks possible like man in the middle attack, chosen plain text attack, chosen cipher text attack, replay attack, repudiation, privileges elevation, differential analysis threats, etc.

To prevent such kind of attacks, Identity based cryptography primitives are used, that are Encryption, Key agreement and Digital Signature.

Before, Identity Based Cryptography (IBE), Public Key Infrastructure (PKI) is used, in which, Certificate Authority is responsible to manage credentials of user through certificates. CA verifies user's certificate before each communication is started and stored information relevant to user, its misbehavior and all other activities. So, it creates overhead of communication and storage of information for each user.

To solve PKI problem, IBE is introduced, which is a public key encryption mechanism where public key is generated from user mail address or IP address, instead of randomly. The corresponding private key is generated by Private Key Generator (PKG) which has also knowledge of Master Key and that Private Key is given to user. IBE has advantage in key management because key distribution and key revocation are not needed. IBE doesn't require a digital certificate to certify public key.

IBE has basic problem of Key Escrow, in that private key of user is known by PKG. So PKG centre can easily decrypt message and forge signature of any user. There is no privacy or authenticity. Secure channel must be there user and PKG centre [5].

IBE first introduced by Shamir in 1984. But IBE is first implemented and solved by Boneh & Franklin in 2001 based on bilinear map, which prevents system from the Chosen Cipher Text attack in Random Oracle Model. In the same year, Cocks gives another scheme for IBE based on Quadric Residues. Hierarchical IBE was first introduced by Horwitz and Lynn to reduce the work load of PKG centre by defining slave PKGs under the Root PKG centre. A simple Mediated RSA based IBE introduced by Ding and Tsudik [6].

IBE is basically composition of four basic four algorithms. Setup() generates global parameters and a master key. Extract() uses the master key to generate private key from public key ID string. Encrypt() generates cipher using public key ID. Decrypt() decodes cipher using the private key [7].

There are some benefits from the use of IBE, like it makes easy the management of public key and use of private key because sender doesn't require certificate every time to send message. Another is managing users' credentials those are easily granted by KGC. It also doesn't require distribution of public key securely. Third one is Encryption with keyword search, in which if receiver wants to find messages with search keyword, sender simply encrypts that search keyword with message in addition. When message received by receiver, it gets private key for that search keyword and get all the encrypted massages along with that search keyword. It also reduces the computational process of encryption because cryptography is conducted offline, without the Key Generation Centre. Identity Based Encryption changes the process of obtaining public key by constructing one to one mapping between identities and public key [8].

However, one main drawback of IBE is it does not support fine grained revocation of key, because revocation is done through Certificate Revocation List which is not available in IBE.

IBE algorithms are introduced for chosen plain text attack, chosen cipher text attack under random oracle models, use hash functions to generate keys, or without random oracle model, uses different parameters to generate keys.

3. MEDIATED RSA BASED ON IDENTITY

Mediated RSA is improved version of standard RSA public key cryptography technique. It is simple and practical process of splitting RSA private keys between the user and the Security Mediator (SEM). The main idea behind the Mediated RSA is to split the private key. One is given to user and another one is given to SEM. SEM is an online semi-trusted server, an user wants to encrypt or decrypt message, a token must be required to take from SEM. SEM is scalable, that can serve many users. The private key is not held by any one party either SEM or User, which is transparent to the outside. Means who use public key has the knowledge that half private key can be not used to decrypt message [9]

Mediated RSA provides fast and fine-grained control of users' security parameters. Mediated RSA also relies on Public Key Certificates to derive public key. Mediated RSA has simple key revocation scheme, in which administrator instructs the SEM to stop issuing the key to particular user for public key. At that time, that user's encryption/decryption privileges are revoked [10].

Mediated RSA based on Identity provides security based on user identity. For generating public key of recipient, a public key mapping function is used, that is doing one-to-one mapping from identity strings to public keys. It uses single common RSA modulus for all users. This modulus can be public and contained into the public key certificate issued by the Certificate Authority.

The current Identity Based mRSA is working under the assumption that the Security Mediator (SEM) never compromised. We stress that using the same modulus by multiple users in a normal RSA setting is utterly insecure. It is subject to a trivial attack where by any one–utilizing one's knowledge of a single key pair can simply factor the modulus and compute the other user's private key [11].

To send encrypted message, sender first computes exponent from the recipient's Identity value. Then this exponent and modulus will be considered as a public key for RSA and used to encrypt message.

There are basically three algorithms are used, one is key generation by Certificate Authority, then Encryption and Decryption, which are described as follows, [12]

System Setting and key generation

In the initialization phase, a trusted party (CA) sets up the RSA modulus for all users in the same system. First, CA chooses, at random, two large primes p' and q' such that $p=2p'+1$ and $q=2q'+1$ are also prime. Then it computes $n=p \bullet q$, a randomly chosen number in Z_n has negligible probability of not being relatively prime to $\Phi(n)$. The public exponent is set to be the email address represented as a binary string. It is assumed that the email address is at most 8 bits shorter than the size of the RSA modulus. One private key is issuing to the user who wants to decrypt message came from x. And anther private key issues to the SEM server. A domain or system wide certificate is issued by the CA after completion of this algorithm. That certificate contains common part of mail address and the common modulus for all users.

Encryption

To encrypt the message, sender needs recipient's mail address and its organization certificate. From the certificate sender can retrieve the common modulus. Here, actually the certificate is not required for the encryption process or to ensure that intended receiver is correct public key holder or not. If any user needs to be revoked, the administrator notifies the appropriate SEM not to issue public or private key of that to be revoked user to any user.

Decryption

The decryption process is identical to Mediated RSA. In which, the receiver first request SEM to send another half private key to him. After receiving request, SEM checks that receiver is valid or not by checking it's certificate. If that receiver is not revoked then, SEM calculates its private key and sends to user. Concurrently, user also calculates its private key. Then by combining both private keys, user decrypts encrypted message.

This current system Mediated RSA based on Identity has potential problems like CA is required to verify

certificates, management overhead of certificate revocation. If assumption relevant to SEM is wrong then system can be unstable also.

4. PROPOSED SYSTEM

The proposed System, Identity Based Encryption with Mediated RSA (IBE-mRSA) is to provide the better security to the data in Software-as-a-Service of Cloud Computing. IBE-mRSA will provide integrity and confidentiality to the communication system in SaaS Cloud. It is based on Public Key Encryption algorithm Mediated RSA and Basic Identity Based Cryptography scheme.

IBE-mRSA scheme is designed to prevent Indistinguishable Identity Chosen Cipher text, Indistinguishable Identity Chosen Plain text attack, Denial of Services by providing integrity and confidentiality.

This IBE-mRSA scheme uses bilinear mapping of two large prime numbers from the two sets of prime numbers. It has also four functions setup, key generator, encryption and decryption as follows.

Setup ( )

It uses a single hash function. It takes Identity of Receiver and random master key. Setup function has,

- Take random $s \in \mathbb{Z}_q^*$, which is master key of prime order q.
- Public Key P_{id} is defined as

$$P_{id} = s \bullet H(ID_r)$$

Output is Public Key P_{id}.

Keygen ( )

In Key Generation, keygen, procedure takes the public key from the setup procedure and generates the private key for the Security Mediator (SEM) and user who receive the message. It is based on the Standard RSA procedure,

- Let k be the security parameter
- Generate random k/2-bit primes, p′ and q′ such that $p = 2p' + 1$ and $q = 2q' + 1$ are also prime.
- $n \leftarrow pq$, $e \in_R \mathbb{Z}^*_{\emptyset(n)}$, such that

$$d \leftarrow e^{-1} \bmod \emptyset(n)$$

- For each user (x),
  - $s \leftarrow k - |P_{id}| - 1$
  - $e_x \leftarrow 0^s \,||\, P_{id} \,||\, 1$
  - $d_x \leftarrow 1 / e_x \bmod \emptyset(n)$
  - $d_{x,u} \leftarrow Z_n \oplus 1 - \{0\}$
  - $d_{x,sem} \leftarrow (d - d_{x,u}) \bmod \emptyset(n)$

Output will be Private Key for user and Security Mediator, security parameter, modulus n.

Encryption ( )

In Encryption procedure, it takes the Public key from setup function and modulus and exponent from the key generator procedure. Using the public key it will calculate exponent at encryption time. And that exponent and modulus will be considered as a public key just like IB-mRSA, which will be used to encrypt the message.

Public Key Pid, Security Parameter k and Modulus n are taken as input.

- Retrieve P_{id} from Setup procedure.
- $s \leftarrow k - |P_{id}| - 8$
- $e \leftarrow 0^s \,||\, P_{id} \,||\, 1$
- Encrypt message m with (e, n) using standard RSA technique.

Output will be Encrypted Message m′.

Decryption ( )

In Decryption procedure, when user receives the encrypted message, he requests to the SEM to send private key by sending encrypted message. SEM checks the user if he is revoked. If not, then SEM replies with private key for that user. In parallel, user also calculates own private key. After receiving the private key, user combines both private key and decrypts the message.

It is taking input a Encrypted Message. Then it proceeds with following procedure.

- User m′ = encrypted message
- User sends m′ to SEM
- In parallel,
  - SEM:
    - *If USER revoked return (ERROR)*
    - $PD_{sem} \leftarrow m'^{dsem} \bmod n$
    - *Send PD_{sem} to USER*
  - USER:
    - $PD_u \leftarrow m'^{du} \bmod n$
- USER: $M \leftarrow (PD_{sem} * PD_u) \bmod n$
- USER: *If succeed, return (m)*

It gives output a Decrypted Message m.

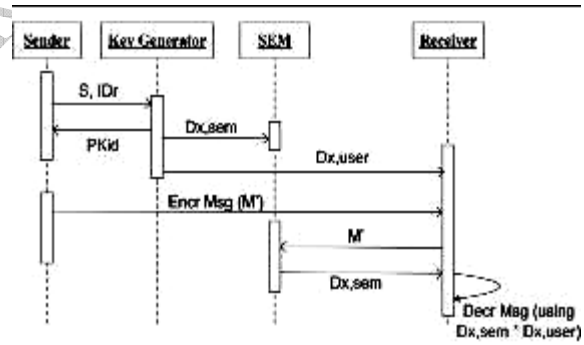

Fig.3 Sequence of Operations in IBE-mRSA.

In the proposed system, the Key Escrow Problem of IBE in Cloud Environment has been solved by dividing key between the SEM and user. And SEM and user never cheat one another also because both don't have the knowledge about each other's key.

The Public Key Infrastructure will not be required for the key mapping functionality in the proposed system. So, certificate verification process will not be required that decreases the computational time, which is potential advantage of proposed system.

5. CONCLUSION

The proposed system works in SaaS environment of Cloud, which increases integrity, efficiency and performance of cryptographic process. It solves the potential problem Key Escrow of IBE as a division of private key between SEM and User. This system will

not require Public Key Generator continuously during communication. It makes easy key revocation process for users. It will work under the random oracle model. But, it should not be cleared that it will work without random oracle model or not such that computation time can be reduced more. As well as, the key generator function takes more time than standard RSA technique.

6. REFRENCES

[1] Kazi Zunnurhain, Susan V. Vrbsky, "Security in Cloud Coumputing", International Conference on Security and Management (2011).

[2] Juhi Sharma, Kshitiz Saxena, "Cloud Security Challenges", International Journal Computer Science and Information Technologies (2012), Vol. 3(3), 4514-4515.

[3] N. Sainath, Vikram Narayandas, S. Jaykrishna, N. Aravind, "Analysis of Cloud Computing Security Considerations for Infrastructure as a Service", International Journal of Engineering Research and Application (IJERA) (2012), Vol. 2(2), 451-456.

[4] Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review", Journal of Emerging Trends in Computing and Information Science (2012), Vol. 3(3), 390-394.

[5] Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangojo Kim, Jeongmo Yang, Seungjae Yoo, "Secure Key Issuing in ID-Based Cryptography", Australasian Information Security Workshop (2004).

[6] M. Chaudary Gorantla, Raju Gangishetti and Ashutosh Saxena, "A survey on ID-Based Cryptographic Primitives"

[7] Dan Boneh and Mathew Franklin, "Identity-Based Encryption from the Weil Pairing", SIAM J. of Computing (2003), Vol. 32(3), 586-615.

[8] Alexandra Boldyreva, Vipul Goyal, Virendra Kumar (2008), "Identity-based Encryption with Efficient Revocation", 14th ACM Conference on Com-puter and Communications Security

[9] Sherman S.M. Chow, Colin Boyd, Juan Manuel Gonz´alez Niet, "Security-Mediated Certificate-less Cryptography".

[10] Satoshi Koga, Kenji Imamoto, Kouichi Sakurai, "Enhancing Security of Security-Mediated PKI by One-time ID".

[11] Xuhua Ding, Gene Tsudik (2003), "Simple Identity-Based Cryptography with Mediated RSA", CT-RSA LNCS 2612, Pages 192-209.

[12] Dan Boneh, Xuhua Ding, Gene Tsudik, "Identity-Based Mediated RSA".