IDENTITY BASED MEDIATED RSA IN SECURE CLOUD COMPUTING

Preeti Kakkar 1, Kapil Kumar 2

1,2 Department of Computer Science and Engineering, GRD Institute of Management and Technology, Uttarakhand Technical University, Dehradun, India

ABSTRACT:

We are living in a technology-enabled application generation and the possibilities are endless. Several companies have been carrying out R&D to make most of cloud technology. In this paper, we display that IB can be used for a type of application that we term "attribute-based encryption". We present constructions of IB_mRSA schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose identity. Proposed scheme is ID-based, but without any assumption of pre-fixed trusted relationship between users and PKG, which effectively solves the problem that exists in some existing ID-based public key cryptosystems in which a trusted PKG and key escrow are needed. Further the proposed technique involves combining the Identity Based Scheme with Mediated RSA for a secure functioning of cloud. This aligns well with the idea of cloud computing to allow the users with a platform of limited performance to outsource their computational tasks to more powerful servers. We have further implemented the proposed algorithm using Microsoft Visual Studio 2010 Ultimate.

Keywords: Cloud Computing, Data Sharing, Data Storage, Identity-based System, Mediated RSA, Query, Security, SEM.

[1] INTRODUCTION

[1.1] DEFINING CLOUD COMPUTING

Cloud computing model as described by NIST[1] is “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., Networks, Servers, Storage, Applications, and Services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Cloud Computing is very much cost effective and hence flexible in terms of technology. It is widely known in present day context for its Reliability, Scalability and Affordability.

According to a survey [2], 7 out of 10 people are directly or indirectly connected to the cloud. Today Cloud Computing is well known for touching all periphery of technology with its on-demand and elastic capability. Cloud Computing is gradually and seemingly transforming the Business and Government, and hence exploring the new challenges to the Security. The scenario has been changed from the Server based to the Service based infrastructure. In a cloud environment the Technologies and Applications are delivered
exponentially faster than ever. These new paradigms in the field of IT have introduced new Threats to Security that are still prevailing and emerging.

[1.2] TOP THREATS TO CLOUD COMPUTING

According to the annual report of Cloud Security Alliance 2013 [3], these articles reflect the current agreement among experts about the most significant threats to the cloud security.

[1.2.1] DATA LOSS OR LEAKAGE

The data is open for all in the cloud. As this is the main advantage of cloud computing but it leads to the data compromise. It can be done due to several reasons like lack of Authentication, Authorization and Audit (AAA) control. It also amplifies due to the increase in the number of users day-to-day.

[1.2.2] SECURITY BREACH

In this particular section the intrusions and attacks by the intruders by moving to the cloud are discussed. The security methodology used by the cloud is much more secured and tested than those used in the standalone storage etc. It is quite easier for the administration to block the data which is likely or to be hacked by the intruders. In addition to this the organizations can implement security by the third party rather than using their internal security module. Data confidentiality is the main worry for the cloud users. Many cloud users have adopted “Private Cloud” approach for the sake of securing their private information.

[1.2.3] ACCOUNT OR SERVICE TRAFFIC HIJACKING

There are many methods like phishing, fraud, and exploitation that still prevail to hijack any server. Passwords and credentials are mostly repeated which supports this kind of attack.

[1.2.4] MALICIOUS URLS

Now-a-days hacking is not just limited to the phishing and frauds. It has a new weapon called Social Engineering. Malicious URLs are the key weapon for a social engineer. There are various methods used in detecting the malicious URLs. Xin (Robert) Luo et al. [4] describes the human factors that help the social engineers. This article examines human factors that can lead to social engineering intrusions. They have focused on a machine learning solution that identifies malicious URLs using a combination of URL lexical features, and JavaScript source features. Monther Aldwairi & Rami Alsalman[5] uses the Naive approach for the detection process for the authenticity of the URL under scanner. Justin Ma et al. [6] also highlighted in their paper a model that helps in and automatically analyzing tens of thousands of features potentially indicative of suspicious URLs.
[1.2.5] INSECURE INTERFACES AND APIs

The interfaces and the different APIs are open to the users for the communication among the different services. The security and the availability of the services highly depend on these interfaces and APIs. There are many activities like encryption, authentication and access control mechanism that are monitored by these APIs.

[1.2.6] MALICIOUS INSIDERS

This is a very common attack for any organization. The main cause is the lack of transparency among the customers and the system. The introduction of IT and the management tool under the same roof leads to this problem.

[1.2.7] SHARED TECHNOLOGY ISSUES

Several vendors deliver their services in a highly scalable way by sharing the infrastructure. It is quite obvious that the elements that incorporate this so called infrastructure (e.g., CPU and GPUs) are not kept isolated to match with the multi-tenancy architecture.

[1.3] IB_MRSA IN CLOUD

This paper will reconnoiter how IB_mRSA aspects in cloud and will review current literature on the area. Present and probable applications of IB_mRSA will be explored. Jobs of IB_mRSA will be assessed and we shall also propose future work in the area. Compared with most widely used public-key cryptography, this reduces the complexities of the encryption process. An added advantage seems to come when a message recipients doesn't need advanced preparation or specialized software’s to read the communication system.

We will then consider Digital Signature Schemes and the Identity Based Signature Scheme in particular. Firstly though, we will assess the most common key management systems. Identity-based (IB_mRSA) is a kind of public-key cryptography wherein a third-party secure server uses a simple identifiers, for example an e-mail address, which generates a public key that is further used for encryption and decryption of electronic messages. Information security can be viewed as including three functions: Access control, secure communications, and protection of private data. Information security is also defined as the protection of private data and processing from unauthorized observation, modification, or interference, describes several information security concepts that apply to all information security research specific to cloud computing.

One promising solution to such difficulties is identity-based cryptography or identity-based encryption (IBE). In certain processes, which can be started by the sender, a unique identifying identifier of the recipient (in case his e-mail address) is used for calculating a public key. A trusted third-party secure server, called the private-key generator(PKG), uses any cryptographic algorithm for calculating the corresponding private keys from the public key system. In this way, recipients are able to generate their own secure private keys directly.
from the server when needed, and there is no such worry about distributing these public keys generation for cryptoanalysis for the conversation.

[1.4] IB_MRSA FOLLOW

The success of IBE depends upon this third-party IBE server which generates private keys. The sole information this server stores for permanent duration is a secret master key – it is a large random number which is exclusively distributed to the security domain. This server uses same key to generate a common set of public-key parameters (which includes the server's address) that are provided to every user who installs the IBE software, and thereby recipients' private keys as per requirement.

When the senders create any encrypted message, the IBE software on their systems uses three parameters for public key generation of the message: a start value, the current week number and recipient's identity (usually the e-mail address). Because calendar references are included, the public key that is generated shall automatically expire. A user who has not used this process before can request and receive an IB-encrypted e-mail message upon authentication and a private key that allows to decrypt all e-mails which were encrypted using the user's e-mail address as the public key.

[2] RELATED WORK

Dimitrios Zissis and Dimitrios Lekkas [7] showed that the recent emergence of cloud computing has drastically altered everyone’s perception of infrastructure architectures, software delivery and development models. From a security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. As a result the aim of this paper is twofold; firstly to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposed introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. Security in a cloud environment requires a systemic point of view, from which security will be constructed on trust, mitigating protection to a trusted third party.

Paras Yadav et al. [8] showed that cloud computing is a new computational paradigm that offers an innovative business model for organizations to adopt IT without upfront investment. In this paper, they discussed security issues for cloud computing. They investigated the problem from the cloud architecture perspective, the cloud offered characteristics perspective, the cloud stakeholders’ perspective, and the cloud service delivery and deployment model models perspective. Based on this analysis, they elaborate the numerous unresolved issues threatening the cloud computing adoption and diffusion affecting the various stakeholders associated with it. Based on this discussion we recommend that cloud computing security solutions should: Focus on the problem abstraction, using model-based approaches to capture different security views and link such views in a holistic cloud security model.

Rabi Prasad Padhy et al. [9] analyzed the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to
leverage cloud service to improve their bottom line in this severe economic climate. In this paper, they first discussed various models of cloud computing, security issues and research challenges in cloud computing. Data security is major issue for Cloud Computing. They believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture.

Ravi J. Khimani [10] proposed a system which can be used to prevent data from man-in-the-middle attack, chosen plaintext, chosen cipher text, denial of service attacks. This proposed technique is combination of Identity Based Encryption (IBE) and Mediated RSA (mRSA) techniques for Cloud environment. The proposed system works in SaaS environment of Cloud, which increases integrity, efficiency and performance of cryptographic process.

Xiaofeng Wang and Shangping Wang [11] proposed an efficient ID-based mediated signature scheme without trusted PKG is proposed. Compared with the other schemes, the proposed scheme has other property besides achieving immediate revocation of a signer’s ID. That is, proposed scheme is ID-based, but without any assumption of pre-fixed trusted relationship between users and PKG, which effectively solves the problem that exists in some existing ID-based public key cryptosystems in which a trusted PKG and key escrow are needed. They improved an ID-based signature scheme and constructed an efficient ID-based mediated signature scheme from the bilinear pairing.

Kapil Patel [12] analyzed different schemes used against different attacks under the different strategies. To provide better key management, IBE uses the Private Key Generator (PKG), instead of CA, generates Private Key from the Identity of user. It uses the Hash Functions to provide better security. Identity Based Encryption (IBE) is used for the encryption and digital signature. IBE provides the better security against the different attacks by intruder. In IBE, the key management is easy than the standard Public Key Infrastructure.

[3] PROPOSED MODEL AND ALGORITHM

[3.1] INDENTITY BASED ENCRYPTION IN CLOUD

As we are aware that cloud is very enthusiastically used to store huge amount of data and for data transfer, and security becomes a major concern to this data. Intruder can attack the data or devices or even harm the system in many ways.

There are a number of feasible attacks possible like chosen plain text attack, man in the middle attack, replay attack, chosen cipher text attack, repuditation, differential analysis threats, etc.

To Prevent such kind of attacks, Identity based Cryptography primitives is a huge success. Before Identity Based Cryptography, Public key Infrastructure (PKI) were used, where Certificates Authority manages the credentials of the user. CA is used for verification of certificates of each user before communication is started and stores the information relevant to the user. But this method creates an over head of the communication and storing information each time.

To solve such issues of PKI, IBE was introduced which is a public key encryption mechanism. In IBE the public key is generated from user’s unique identity, such as email...
address, telephone number etc. Then the corresponding private key is generated by the Private key Generator (PKG) which keeps the master knowledge with itself. Now IBE has an added advantage over PKI that no key revocation is needed and IBE even does not needs the digital certificate to certify the public key.

But IBE has a problem of Key Escrow, in that the private key of the user could be known by the PKG, and the PKG centre can easily any time decrypt the messages. IBE has main four algorithm SETUP, EXTRACT, ENCRYPT, DECRYPT. There are some termed benefits of using IBE over any other technique, like it makes management of public key easier and use of private key beneficial because the sender does not need certificate all the time while sending the message. Managing user credentials are easily granted as it does not require the distribution of public key securely.

However, there is one major drawback of using IBE that it does not support fine grained revocation of key because that is done through Certificate Revocation List which is not in the IBE.

Mediated RSA is an improved version of standard RSA because it splits RSA private keys between user and Security Mediator (SEM). The Key is split, where one is given to the user and other to the SEM. The private key here is not held by any one party, and cannot be transparent to the outside world. The one who has the knowledge of half private key cannot use this to decrypt messages. Mediated RSA is also a simple key revocation scheme which can overcome the disadvantage of IBE.

Mediated RSA with Identity Based Encryption provides the security on unique user’s identity. For generation of the public key of user, mapping function for public key is used, that maps the identity onto numbers and finally to public key.

The Current module assumes that Security Mediator (SEM) shall naver be compromited. To send the encrypted message, sender first computes the exponent from recievers’s unique identity value. Then the modulus and exponent is generated which act as public key for RSA and is used to encrypt the message. In our module we have three steps to procedure, Key Generation, Encryption and Decryption.

[3.2] ALGORITHM FOR IB_MRSA KEY GENERATION

The identity also undergoes the setup function wherein the identity i.e email address is converted into numeric numeric which enables the generation of public key.

1. Take a random master key s of prime order q.
2. Public Key $P_u$ is defined using a single hash function.
3. A security parameter k is taken.
4. Random k/2 bit prime p and q are generated
5. A random number and a exponent is generated.
6. For each user
   \[ s = k - |P_u|^{-1} \]
   \[ e_s = 0 || |P_u| || 1 \]
   \[ d_s = 1 / e_s \mod \Phi(n) \]
   \[ d_{u,sem} = \text{private key for user} \]
   \[ d_{u,sem} = \text{private key for sem} \]
[3.3] ALGORITHM FOR IB_MRSA ENCRYPTION

In this procedure, the public key from modulus and setup function and exponent from key generation procedure is taken. Using the public key it calculates the exponent and modulus which shall be further used to encrypt message.

1. $e \rightarrow IB\_mRSA\.key(\text{unique identity})$
2. Message $m$ is encrypted using standard RSA encryption with $(e; n)$ as the public key

Note: The recipient’s public key certificate is not required for the sender to encrypt. The key is derived from the receiver’s unique identifier, the sender does not need a certificate to ensure that the intended receiver is the correct public key holder. Furthermore, instantaneous revocation provided by mRSA obviates the need for the sender to perform any revocation checks.

[3.4] ALGORITHM FOR IB_MRSA DECRYPTION

In this process, when the user receives the encrypted message, he sends request to the SEM to send private key by sending encrypted message. In parallel the user calculates its own private key. After this receiving of keys, the user combines them and decrypts the message.

1. USER: $m' \rightarrow$ encrypted message with cipher text.
2. USER: send $m'$ to SEM with 50% key.
3. In parallel: convert the key split number in bit key.
   - SEM: Split the key number with random number.
   - If USER revoked return (ERROR) on ad-hoc network.
   - $PDsem \rightarrow m^{\text{dx,sem}} \mod n$.
   - Send $PDsem$ to USER with sharing path
4. USER: hold the split key
   - Generate the local cloud
   - Create with data centric approach
   - Receiver decrypt the message
5. $PDu \rightarrow m^{\text{dx,u}} \mod n$
6. USER: $m \rightarrow (PDsem \ast PDu) \mod n$
7. USER: return (m)
   - Revoke the message with cipher text

Thus IB-mRSA provides identity-based encryption along with revocation. Also usage of mRSA decryption technique gives security to the message.

[4] IMPLEMENTATION AND RESULTS

The running module of the proposed system has been implemented using Microsoft Visual Studio 2010 (Visual C# language) which is considered a very familiar programming language with great support of GUI and cloud computing environments. There are possibilities...
Identity Based Mediated RSA In Secure Cloud Computing

to efficiently increase or decrease the type, number, and quality of services according to the needs of various users.

Before starting the system, a few settings on the systems have to be done, and the systems have to connect into a security less combination, so that IB_mRSA functionality can be shown.

The main window of the proposed system is illustrated in Figure.1. This window shall automatically appear when the system is initiated.

![Figure.1. Main window](image1.png)

The main window contains two logins one for the users, and another for the admin. If the admin is logging into the system he has to use the admin button and next window shall open wherein the admin can add new users by authenticating them. The admin window is shown in Figure.2.

![Figure.2. Admin login window](image2.png)

Whenever the user chooses user button to login, he/she gets the user panel wherein the user has to take permission from the admin to login for data transfer. Figure.3. shows the user login window. The authentication of the user is given by the fact that user names chosen by the working system are the MAC address of machine which cannot be forged at any moment during the data transfer.

![Figure.3. User login window](image3.png)
Next once the user login to system he/she is taken to another window wherein there are options of key generation, encryption and decryption as shown in Figure 4.

![Figure 4. Message transfer window](image)

[4.1] PERFORMANCE AND RESULT EVALUATION

In the proposed model, key escrow problem of IBE for cloud environment has been solved. The division of key between the user and SEM provides a better functionality as they both don’t have each other’s knowledge. So they at any point cannot get each other’s keys. The mapping functionality is not required in the proposed system because Public Key Infrastructure is not used. So, here certificate verification is also not required which in turn decreases the computational time, which is a potential advantage of the system.

The results of the key generation have been evaluated and results of RSA are larger than those of the IB_mRSA and the IB_mRSA in cloud, because the key generation of the RSA involves the prime key generation whereas IB_mRSA and the IB_mRSA in cloud is for each user, so it does not involve prime key generation.

The encryption time is increases slightly with the increase in key length, so these key lengths are not problematic. This can be seen in encryption times of the IB_MRSA and IB_MRSA in cloud although the key of the IB_MRSA in cloud is larger than that of IB_MRSA by the value of steps, the times are almost same.

The decryption times are longer than encryption times in all these schemes. These drawbacks are actually inherited from RSA, because these decryption keys are extremely large (length n). The time consumed by all the schemes is proportional to the modulus size. Table 1. Timing Results shows these results. These results are in ms.
Identity Based Mediated RSA In Secure Cloud Computing

We have also evaluated the results of our model with respect to elapsed time. These results show that with the increase in key size the elapsed time also increases. So, smaller the key size time taken for IB_mRSA is also small. This can be seen in the following Figure.5. Key size for IB_mRSA performance in elapsed time.

We have also evaluated the results of our module with respect to elapsed time. These results show that with the increase in modulus size with key size the elapsed time also increases. The module performance degrades when the message size increases more than 2048 bits. This can be seen in the following Figure.6. Module Evaluation for IB_mRSA with respect to elapsed time.
[6] CONCLUSION

The Proposed model shall work in the SaaS environment of network by increasing the performance and efficiency of the process. This scheme solves the problem of Key Escrow of IBE by effectively dividing the private key SEM and user.

The system does not use Private Key Generator all the time during communication. The scheme works well under random oracle model. This scheme can be assigned to data centric in cloud computing, and shall combine the data security approach in disconnected environment also, which is main merit of the application using network login with secure mediated key by taking identification for network using MAC name.

[7] ACKNOWLEDGEMENT

The author gratefully acknowledges the help of Mr. Kapil Kumar for supporting to research on the topic and guidance. Moreover is obliged for his help in the final language editing of this paper.
REFERENCES


