Trusted Security Model for User’s Data for Public Cloud Using RSA Encryption

Pallavi Pandey¹, Priyanka Dhasal², Rakesh Pandit³
¹M.Tech Scholar, ²HOD, ³Professor, IT Department, Patel College of Science and Technology, Indore, India

Abstract— Now, a day’s Cloud Computing concepts are new paradigm for researchers and software industry. Cloud computing providing people the way to share distributed resources and services that belong to different organizations or sites. By providing distributed resources via the network in the open (public) environment, having different types of issues, securing user’s data is one of them for trust on open cloud environment. In this paper, proposed a cloud model to build a trusted computing and data environment for cloud computing system. We propose a model system in which user’s data is encrypted at user’s side and will save at cloud remote database end. This model has important security services, including authentication, confidentiality and integrity.

Keywords - Cloud computing; RC algorithm, Remote database, trusted computing platform; trusted service.

I. INTRODUCTION

Cloud computing, a new kind of computing model. It is an extend of changing with the need. With the rapid development of the Internet, user’s requirement is realized through the Internet, different from shifting with the need. In fact cloud computing is an extend of grid computing, distributed computing, and parallel computing. Its foreground is to provide secure, quick, well-situated data storage and net computing service centered by internet.

The characteristics of cloud computing is the virtualization, distribution and dynamically extendibility. Virtualization is the key quality. Most software and hardware have provided carry on to virtualization. By virtualization, many factors such as IT resource, software, hardware, operating system and net storage, can manage in the cloud computing platform; every environment has nothing to do with the physical platform.

A. Cloud Computing Principle

Computing is a virtual group of computing resources. It provides computing resources in the pool for users through internet. It provides a compulsory application program environment [4].

It can deploy, allocate or reallocate computing resource dynamically and keep an eye on the usage of resources. Cloud computing collects all the computing resources and manages them automatically through software.

B. Cloud Computing Applications and Advantages

1. Cloud computing do not necessitate high quality equipment for user, and it is easy to use.
2. Cloud computing provides trustworthy and secure data storage center. No Need to worry the harms such as data loss or virus [18].
3. Cloud computing can realize data sharing between different equipment’s.
4. Cloud provides nearly infinite possibility for users to use internet.

C. Cloud Computing Issues

There are different security issues in cloud. It is showing in Figure 1. Issues are as following:

1) Trust: Now under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the service provider.

2) Security: In the leading edge cloud services provider will employ data storage and transmission encryption, user authentication, and authorization (data access). Many users worry about the vulnerability of remote data to such criminals as hackers, thieves, and disgruntled employees. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigating concern.

3) Identity Management: Data sensitivity and privacy of information have increasingly become a concern for organizations, and unauthorized access to information resources in the cloud is a major issue.

4) Data Backup: Cloud providers employ redundant servers and routine data backup processes, but some people worry about being able to control their own backups.
5) **Ownership:** Once data has been relegate to the cloud, some people worry that they could lose some or all of their rights or are unable to protect the rights of their customers. Many cloud providers are addressing this issue with well-crafted user-sided agreements. Users would be wise to seek advice from their favorite legal representative.

6) **Visibility:** Migration to cloud services relinquishes control to the service provider for securing the systems on which the organization’s data and applications operate. To avoid creating gaps in security, management, procedural, and technical controls must be applied commensurately with those used for internal organizational systems.

7) **Risk Management:** The cloud is relatively uncharted territory in terms of risk management and compliance, particularly when institutional data will be stored and processed in the cloud. Campus data is increasingly being stored and processed by third parties that might have different security and compliance analysis procedures than were developed for institution-based data services.

3) **Storage Server:** It is a server in which the data were stored in a cloud. This data may be transfer to data center in another country.

4) **Audit and monitoring:** To maintain operation assurance organization use to basic method:

   a) **System Audit**
   b) **Monitoring**

   System audit is a one time or period event to evaluate security. IT Auditors audit the following main function:
   - Systems development standard
   - Backup controls
   - Data center security
   - Data library procedure.
   - Transactions controls

   Monitoring refers to as ongoing activity that examines either the system or the users.

III. **SOLUTION FOR SECURITY AS MAJOR ISSUE**

To preventing the system from outside world, so that no one can damage or change the system and system can serve its services continuously. The most damaging aspect is the loss of data and software. Some of sources for damaging the systems are computer viruses, computer hacking and denial of service attacks, have become more common.

Cloud Storage system provides the user for safe and consistent place to save valuable data and documents. User's files are not encrypted on some open source cloud or public storage systems while uploading. Data/file is encrypted as per provider. So, the storage service provider can easily access the user's files or misuse the data. This brings a big concern about user's privacy. The user has no supreme control over the software applications including secret data.

User has to depend on the provider’s action, maintenance and admin it. The user does not have direct access to the software to fix the problems while something goes wrong in any application and its valuable data.

The cloud authentication for Digital Signature with RSA algorithm scheme is to guarantee the security of data in cloud. RSA is maybe the most recognizable asymmetric algorithm. RSA was created by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. Till now, it is the only asymmetric i.e. needs two different keys algorithm used for private/public key generation and encryption. To enhance the security of cloud computing both digital signature scheme and public key cryptography are used.
By using RSA encryption in cloud computing environment, overcome the problem, it is also enhancing the data transmission security. Data is encrypted before transmission, so that corresponding keys cannot be restored, even if the data is stolen. Only the user knows the key, cloud does not know the key. Also the properties of encryption, the cloud can operate on cipher text, thus avoiding the encrypted data to the traditional efficiency of operation. User's privacy is protected because user's files are encrypted in cloud storage.

Initially at cloud user end, selecting the file for encryption, which is using encryption password and number of rounds. Then user can store file at remote storage.

An RSA public-key/private-key pair can be generated by the following steps:

1) Create a pair of large, random prime’s p and q from cloud client.
2) Compute the modulus n as n = pq.
3) Select an odd public exponent e between 3 and n-1 which is relatively prime to p-1 and q-1.
4) Work out the private exponent d from e, p and q.
5) The cloud output (n, e) as the public key and (n, d) as the private key.

The encryption operation in the RSA cryptosystem is exponentiation to the eth power modulo n:

\[ c = \text{ENCRYPT} (m) = me \mod n. \]

For existing cloud the input m is the message; the output c is the resulting cipher text.

The actual message is encrypted with the shared key using a traditional encryption algorithm.

At the cloud storage access end, the decryption operation is exponentiation to the dth power modulo n:

\[ m = \text{DECRYPT} (c) = cd \mod n. \]

A message can be digitally signed by applying the decryption operation to it, i.e., by exponentiating it to the dth power:

\[ s = \text{SIGN} (m) = md \mod n. \]

In practice, the plaintext m is generally some function of the message, for instance a formatted one-way hash of the message.

The goal of this work is to implement a RSA encryption algorithm in cloud environment that can be used in cloud services. User must trust on cloud for storage sensitive data and file, and it can also encrypt his data according to their need.

IV. CONCLUSION

Here data security problems in the cloud system are discussed. Cloud computing has a very fast pace of development and shows good prospects and great potential. The cloud computing is related to many areas of information management and services. The data privacy issue becomes more prominent than the traditional network because the data in the cloud computing environment is greatly dependent on the network and server. There are many customers who mistrust the security and privacy of cloud computing customers and they do not want to move the data into the cloud platform.

REFERENCES