Providing Data Security in Cloud Computing using public key cryptography

N.PADMAJA¹, PRIYANKA KODURU²

¹ Department of Information Technology, School of Engineering & Technology, SPMVV, Tirupati
² Department of Computer science & Engineering School of Engineering & Technology, SPMVV, Tirupati

¹gowrapadma@yahoo.com, ²kodurpriyanka@gmail.com

ABSTRACT
Cloud Computing is a new technology in computer oriented services. No secret that cloud computing is becoming more and more popular and is ever increasing due to fast growth in the field of “cloud computing” increases serious security concerns in the large companies as they share valuable resources in a cost effective way. Due to increasing demand for more clouds there is a security threat, these security threats can be a danger to cloud computing and they have to be avoided. Since Cloud Computing stores the data and disseminated resources in the open environment, security has become the major issue which is hampering the deployment of Cloud environments. Even though Cloud Computing is promising and efficient, there are many challenges in data security for the Cloud user. To access a cloud based web application that will try to eliminate the concerns regarding data privacy, segregation. We proposed a method by implementing RSA algorithm.

Keywords— Cloud Computing, Data Security, RSA algorithm, Encryption, Decryption.

1. INTRODUCTION
Cloud computing refers to Internet based development and services. Cloud is simply the trendy term for a network or remote servers that can be addressed via an internet connection store and manage information. The three main aspects of cloud computing are Software as a service (SaaS) is a model of software deployment where an application is hosted as a service provided to customers across the Internet. Oracle CRM on Demand, Salesforce.com and Net suite are some of the well known examples of SaaS. SaaS is generally used to refer business software rather than consumer software, which falls under Web 2.0. By removing the need to install and run an application on a user’s computer it is seen as a way for businesses to get the same benefits as commercial software with smaller cost outlay. SaaS also make it less intense of the burden of software maintenance and support, but users relinquish control over software versions and requirements. The other terms that are used in this sphere include Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The pioneer of cloud computing vendors are Amazon Simple Storage Service (S3) and Amazon Elastic Compute cloud (EC2) are well known examples of cloud computing.

Cloud computing is the key driving force in many companies hence, the major concern in the cloud computing is providing the security of their data in the cloud. Securing data is more important because of the critical nature of cloud computing and the large amounts of complex data it carries concerns regarding data privacy and security are proving the broader uptake of cloud computing services. Open source clouds such as the Ubuntu cloud offer smaller businesses a chance to try the benefits of cloud.

[Diagram showing Cloud computing services: SaaS, PaaS, IaaS]

Cloud facilitates development and deployment of applications without the cost complexity of buying and managing the underlying infrastructure providing all of the facilities required to support the complete life cycle of building and delivering web applications. The most popular cloud types are private, public and hybrid clouds. In a private cloud, the infrastructure for implementing the cloud is controlled completely by the enterprise. Private clouds are implemented in the enterprise’s data centre and managed by internal resources and maintains
all corporate data under the control of the legal and contractual umbrella of the organization. The cloud data security depends on appropriate data security measures and procedures, as many companies move their data to the cloud, data may undergo many changes and there are many challenges to overcome. Computer-based security measures mostly capitalize on user authentication and authorization.

2. DATA SECURITY ISSUES IN THE CLOUD

The security issue with clouds is that the data may not have control of the data is placed. As if user wants to take advantage of the cloud, user must ensure the safe network and also utilize the resource allocation and scheduling provided by clouds. The secured data exchange is crucial for any network; so it is very important to take security and privacy into account when designing and using cloud services. Cloud Computing is enlarged way to cover security issues, concerns and challenges for Data Security in Cloud.

2.1 Cloud Privacy and Confidentiality:

Confidentiality is defined as the sensitive information is not disclosed to unauthorized persons, processes, or devices. The service provider knows where the users' confidential data is located in the cloud computing systems. Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to sensitive data by cloud personnel is another risk that can pose potential threat to data in cloud computing. Assuredness should be provided to the clients for proper practices in privacy policies and procedures to assure the cloud users for the data safety. Cloud service providers should implement mechanisms to ensure data integrity. The cloud provider should make the client aware of what particular data is hosted on the cloud. It may be necessary to have exact records as to what data was placed in a public cloud, when it required, what virtual memories (VMs) and storage it resided on when it was processed, such data integrity requirements exists, that the origin and custody of data or information must be maintained in order to prevent tampering or to prevent the exposure of data beyond the agreed territories (either between different servers or different networks).

2.2 Data Location and Relocation:

Cloud Computing offers a high degree of data mobility. Data mobility is at a high level then the risks and issues increase many folds especially consumers do not always know the location of their data. When an enterprise has some sensitive data that is kept on storage device in the Cloud, users want to know the location of data and also wish to specify required location. The contractual agreement, between the Cloud provider and the consumer data should stay in a particular location or reside on a given known server, cloud providers should take responsibility to ensure the security of systems and provide robust authentication to safeguard customers’ information. Data is initially stored at an appropriate location decided by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others’ resources. For example, emails, photographs uploaded to Face book can reside anywhere in the world and Face book members are generally not concerned. They may also wish to specify a preferred location (e.g. data to be kept in the UK) then requires a contractual agreement between the Cloud service provider and the consumer.

2.3 Storage, Backup and Recovery:

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. Most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.  

3. DATA SECURITY

Data confidentiality and audit ability are the primary hurdles of the cloud computing technology in organizations, according to a recent survey of over 2100 Indian Business Technology professionals (Fig.2).

Fig. 2. Data Security is Top Adoption Obstacle for Cloud in India

The survey conducted by Salt March Intelligence, measured perceptions of Business technology professionals
include their challenges in adopting Cloud in their organizations in different stages of adoption, and cloud platforms, applications, clients, infrastructure and storage used. Financial savings, agility and elasticity, all enabled through cloud technology, are crucial in a fast business world. At the same time security incidents in the Cloud have made clear that this new promising technology comes with complexity and security challenges. "While Data confidentiality and audit ability (24.5%) topped the list of primary obstacles for the use of cloud computing technologies, performance unpredictability (22.1%) appeared to be another key factor dampening adoption levels." Data transfer bottlenecks (18.5%) and data lock-in (15.3%). Information is produced at a rapid rate and more and more openly shared through new and agile collaboration channels that are no longer under control. Data mobility is at a high level then the risks and issues increase especially when data is transferred to another country with different regulatory framework and data relocation have not positive implications for data security, protection and data availability.

The main concern with reference to security of data in Cloud is to ensure security of data that is at same location although, consumers know the location of data and there in no data relocation, there are questions relating to its security and confidentiality of it. Because of the broad network access and flexibility cloud computing becoming more popular. Reliability is in terms of safe and secure environment for the personal data. Cloud computing security is the set of control-based technologies and policies to follow regulatory agreement rules and protect information, data applications and infrastructure associated with cloud computing use.

4. RSA Algorithm

RSA is a Public-Key cryptography algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977 at MIT. RSA algorithm uses the product of two prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret, using RSA algorithm encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it.

<table>
<thead>
<tr>
<th>Table 1: RSA Algorithm securities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To do this</strong></td>
</tr>
<tr>
<td>Send an encrypted message</td>
</tr>
<tr>
<td>Send an encrypted signature</td>
</tr>
<tr>
<td>Decrypt an encrypted message</td>
</tr>
<tr>
<td>Decrypt an encrypted signature (and authenticate the sender)</td>
</tr>
</tbody>
</table>

RSA Algorithm is a asymmetric public key algorithm it uses two different keys one is public key and another is private key this algorithm involves multiplying two large prime numbers that constitutes the public key and private key, once the keys have been developed, the original prime numbers are no longer important and can be discarded. The private key in RSA algorithm never needs to be sent across the internet. Private Key is used to decrypt text that has been encrypted with the public key. RSA is a block cipher, in which every message is mapped to an integer. User data is encrypted first and then it is stored in the Cloud. When required, user places a request the data for the Cloud provider, Cloud provider authenticates the user and delivers data. RSA is a block cipher, in which every message is mapped to an integer. Encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with corresponding private key.

4.1 RSA algorithm involves three steps:

RSA Algorithm uses two keys public and private and which are asymmetric because one is used for encryption and another is used for decryption.

The public-key encryption system has mainly three phases:
1. Key Generation
2. Encryption
3. Decryption

**Key Generation:**

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:
1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute \( n = p \times q \)
3. Compute Euler’s totient function, \( \phi(n) = (p-1) \times (q-1) \).
4. Choose an integer e, such that \( 1 < e < \phi(n) \) and greatest common divisor of e, \( \phi(n) \) is 1. Now e is
released as Public-Key exponent.

5. Now determine d as follows: \( d = e^{-1} \mod \phi(n) \) i.e., d is multiplicative inverse of \( e \mod \phi(n) \).
6. d is kept as Private-Key component, so that \( d \times e \equiv 1 \mod \phi(n) \).
7. The Public-Key consists of modulus n and the public exponent e i.e., (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e., (d, n).

**Encryption:**
Encryption is the process of converting original plain text (data) into cipher text (data).
Steps:
1. Cloud service provider should give or transmit the Public-Key (n, e) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text (data) \( C \) is:
   \[ C = m^e \mod n \]
4. This cipher text or encrypted data is now stored with the Cloud service provider.

**Decryption:**
Decryption is the process of converting the cipher text (data) to the original plain text (data).
Steps:
1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e., C.
3. The Cloud user then decrypts the data by computing, \( m = C^d \mod n \).
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

### 4.1.1. Experimental Results
Sample data for implementing RSA algorithm:

**Key Generation:**
1. We have chosen two distinct prime numbers \( p=17 \) and \( q=11 \).
2. Compute \( n=p\times q \) thus \( n=17\times11=187 \).
3. Compute Euler’s totient function, \( \phi(n)=(p-1)\times(q-1) \) Thus \( \phi(n)=(17-1)\times(11-1)=16\times10=160 \)
4. Chose any integer e, such that \( 1 < e < 160 \) that is co prime to 160. Here, we chose \( e=7 \)
5. Compute \( d \),
   \[ d = e^{-1} \mod \phi(n) \]
   Thus \( d=7^{-1} \mod 160 = 23 \).
6. Thus the Public-Key is \( (e, n) = (7, 187) \) and the Private-Key is \( (d, n) = (23, 187) \). This Private-Key is kept secret and it is known only to the user.

**Encryption:**
1. The Public-Key \( (7, 187) \) is given by the Cloud service provider to the user who wish to store the data.
2. Let us consider that the user mapped the data to an integer \( m=88 \).
3. Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user.
   \[ C = 88^7 \mod 187 = 11 \]
4. This encrypted data i.e., cipher text is now stored by the Cloud service provider.

**Decryption:**
1. When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid).
2. The cloud user then decrypts the data by computing, \( M = c^d \mod n \)
   \[ M=11^{23} \mod 187 = 65 \]
3. Once the M value is obtained, user will get back the original data.

**Conclusion**
Cloud Computing is still a new technology where the cloud services are readily accessible as on a pay-per-use basis. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography. Only the authenticated and authorized user can access the data, even if some unauthorized user gets the data accidentally or intentionally and if captures the data also, user cannot decrypt the data and get back the original data from it. Data security is provided by implementing RSA algorithm. The performance of an algorithm on a cloud network varies according to the type of the algorithm such as symmetric, asymmetric or hashing algorithms and also varies with the size of the input.
REFERENCES