Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing

[#1] Uma Somani, [#2] Kanika Lakhani, [#3] Manish Mundra

[#1] urmisom2005@gmail.com , [#2] kanikalakhani@yahoo.co.in ,

[#3]manishmundra.2010@gmail.com

Abstract The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. Cloud computing is the Concept Implemented to decipher the Daily Computing Problems, likes of Hardware Software and Resource Availability unhurried by Computer users. The cloud Computing provides an undemanding and Non ineffectual Solution for Daily Computing. The prevalent Problem Associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network. In this Research Paper, we have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm

1. Introduction

Cloud computing is the Internet-based development and is used in computer technology. It has become an IT buzzword for the past a few years. Cloud computing has been often used with synonymous terms such as software as a service (SaaS), grid computing, cluster computing, autonomic computing, and utility computing . SaaS is only a special form of services that cloud computing provides. Grid computing and cluster computing are two types of underlying computer technologies for the development of cloud computing.

It is often difficult to define the cloud computing. Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet. It provides a mandatory application programming environment. It can deploy, allocate or reallocate computing resource dynamically and monitor the usage of resources at all times

Cloud computing collects all the computing resources and manages them automatically through software. In the process of data analysis, it integrates the history data and present data to make the collected information more accurate and provide more intelligent service for users and enterprises. The users need not care how to buy servers, software solutions and

978-1-4244-7674-9/10/$26.00 ©2010 IEEE

so on. Users can buy the computing resource through internet according to their own needs. Cloud computing does not depend on special data center, but we can look it as the inevitable product of grid computing and efficiency computing. Cloud computing is easy to extend, and has a simple management style. Cloud is not only simply collecting the computer resource, but also provides a management mechanism and can provide services for millions of users simultaneously. Organizations can provide hardware for clouds internally (internal clouds), or a third party can provide it externally (hosted clouds). A cloud might be restricted to a single organization or group (private clouds), available to the general public over the Internet (public clouds), or shared by multiple groups or organizations (hybrid clouds).

2. Characteristics of Cloud Computing

1 Ultra large-scale: The scale of cloud is large. The cloud of Google has owned more than one million servers. Even in Amazon, IBM, Microsoft, Yahoo, they have more than hundreds of thousands servers. There are hundreds of servers in an enterprise.

2.Virtualization: Cloud computing makes user to get service anywhere, through any kind of terminal. You can complete all you want through net service using a notebook PC or a mobile phone. Users can attain or share it safely through an easy way, anytime, anywhere. Users can complete a task that can't be completed in a single computer.

3 High reliability: Cloud uses data multi-transcript fault tolerant, the computation node isomorphism exchangeable and so on to ensure the high reliability of the service. Using cloud computing is more reliable than local computer.

4 Versatility: Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.

5. High extendibility: The scale of cloud can extend dynamically to meet the increasingly requirement.

6. On demand service: Cloud is a large resource pool that you can buy according to your need; cloud is just like running water, electric, and gas that can be charged by the amount that you used.

7. Extremely inexpensive: The centered management of cloud make the enterprise needn't undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully enjoy the low cost advantage. Various application and advantage of cloud computing are listed below:

1 Cloud computing do not need high quality equipment for user, and it is easy to use.

2 Cloud computing provides dependable and secure data storage center. You don't worry the problems such as data loss or virus

3 Cloud computing can realize data sharing between different equipments.

4 Cloud provides nearly infinite possibility for users to use internet.

3. Cloud Security Challenges

Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing paradigm. This is particularly true for the SaaS provider. Some security concerns are worth more discussion. With the cloud model, you lose control over physical security. In a public cloud, you are sharing computing resources with other companies. In a shared pool outside the enterprise, you don't have any knowledge or control of where the resources run. Exposing your data in an environment shared with other companies could give the government "reasonable cause" to seize your assets because another company has violated the law. Simply because you share the environment in the cloud, may put your data at risk of seizure. Storage services provided by one cloud vendor may be incompatible with another vendor's services should you decide to move from one to the other. Vendors are known for creating what the hosting world calls "sticky services"—services that an end user may have difficulty transporting from one cloud vendor to another. Data integrity is assurance that the data is consistent and correct. Ensuring the integrity of the data really means that it changes only in response to authorized transactions.

4. Security and Responsibility

Within the cloud computing world, the virtual environment lets user access computing power that exceeds that contained within their own physical worlds. To enter this virtual environment requires them to transfer data throughout the cloud. Consequently, several data storage concerns can arise. Typically, users will know neither the exact location of their data nor the other sources of the data collectively stored with theirs. To ensure data *confidentiality*, *integrity*, and *availability* (CIA), the storage provider must offer capabilities that, at a minimum, include a tested encryption schema to ensure that the shared storage environment safeguards all data; stringent access controls to prevent unauthorized access to the data; and scheduled data backup and safe storage of the backup media. Legal issues arise, such as e-discovery, regulatory compliance (including privacy), and auditing .The range of these legal concerns reflects the range of interests that are currently using or could use cloud computing. These issues and their yet-to-be-determined answers provide significant insight into how security plays a vital role in cloud computing continued growth and development...

A. Use in Cyber crime

Cyber crime's effects are felt throughout the Internet, and cloud computing offers a tempting target for many reasons. Providers such as Google and Amazon have the existing infrastructure to deflect and survive a cyber attack, but not every cloud has such capability. If a cyber criminal can identify the provider whose vulnerabilities are the easiest to exploit, then this entity becomes a highly visible target. If not all cloud providers supply adequate security measures, then these

clouds will become high-priority targets for cyber criminals. By their architecture's inherent nature, clouds offer the opportunity for simultaneous attacks to numerous sites, and without proper security, hundreds of sites could be comprised through a single malicious activity.

5. Digital Signature with RSA encryption algorithm to enhance Data Security in Cloud

In Cloud computing, we have problem like security of data, files system, backups, network traffic, host security .Here we are proposing a concept of digital signature with RSA algorithm, to encrypting the data while we are transferring it over the network. .A **digital signature** or **digital signature scheme** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit.

We proposed digital signature with RSA algorithm scheme to ensure the security of data in cloud. RSA is probably 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.We include both digital signature scheme and public key cryptography to enhance the security of cloud computing.

In Digital Signature, software will crunch down the data, document into just a few lines by a using "hashing algorithm". These few lines are called a message digest. Software then encrypts the message digest with his private key. Then it will produce digital signature .Software will Decrypt the digital signature into message digest with public key of sender's and his/her own private key. We are using Digital signatures so that we are able to distribute software, financial transactions, over the network and in other cases where it is important to detect forgery and tampering.

6. Proposed Internal Working Steps Taken in Digital Signature with RSA Algorithm

Let us assume we have two enterprises A and B. An enterprise A have a public cloud with data, software's and applications. .Company B wants a secure data from A's Cloud .We are here, trying to send a secure data to B by using Digital signature with RSA algorithm. We are taking some steps to implementing Digital signature with RSA encryption algorithm.

Suppose Alice is an employee of an enterprise A and Bob is an employee of a company B.

Step1. Alice takes a document from cloud, which Bob wants.

Step2. The document will crunched into few lines by using some Hash function the hash value is referred as message digest.(Figure 1)

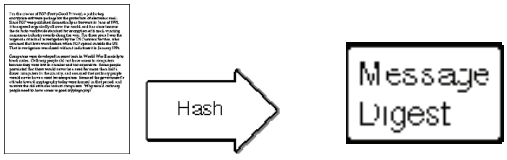

Figure 1 Document crunched into message digest.

Step 3. Alice software then encrypts the message digest with his private key. The result is the digital signature.(Figure 2)

Figure 2 Encryption of message digest into Signature

Step 4. Using RSA Algorithm, Alice will encrypt digitally signed signature with bob's public key and Bob will decrypt the cipher text to plain text with his private key and Alice public key for verification of signature. (Figure 3)

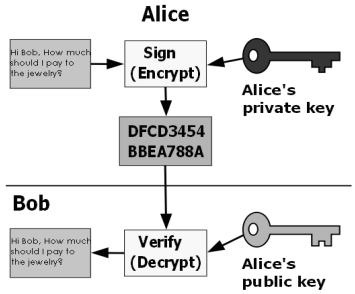

Figure3.Encryption of Digital Signature into Cipher text

7. Proposed Algorithm taken for Implementing Digital Signature with RSA Algorithm

In this algorithm, n is known as the *modulus*. 'e' is known as the *encryption exponent*. 'd' is known as the *secret exponent* or *decryption exponent*.

Step 1. Key Generation Algorithm

1. Choose two distinct large random prime numbers *p* and *q*

2. Compute $n = p\ q$, where *n* is used as the modulus for both the public and private keys

3. Compute the totient: phi $(n) = (p-1)(q-1)$

4. Choose an integer *e* such that $1 < e <$ phi (n) , and *e* and *phi(n)* share no factors other than 1 , where *e* is released as the public key exponent

5. Compute *d* to satisfy the congruence relation $d \times e = 1$ modulus *phi(n)*; *d* is kept as the private key exponent

6.The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

Step2. Digital signing

Sender A does the following:-

A) Creates a *message digest* of the information to be sent by using hash function.

Hash Function

1. Declare character 'str' of unsigned long type.

2. Declare and initialize hash of unsigned integer type

3. unsigned int hash = 0;
   int q;
   while (q = str+1)
   hash =hash + q;

B .) Represents this digest as an integer *m* between 0 and *n*-1

C.) Uses her *private* key (n, d) to compute the signature , $s = m^d \bmod n$.

D.) Sends this signature *s* to the recipient, B.

Step3. Encryption

Sender A does the following:-

1.Obtains the recipient B's public key (n, e).

2. Represents the plaintext message as a positive integer *m*

3. Computes the ciphertext $c = m^e \bmod n$.

4. Sends the ciphertext *c* to B.

Step4. Decryption

Recipient B does the following:-

1. Uses his private key (n, d) to compute $m = c^d \bmod n$.
2. Extracts the plaintext from the message representative *m*.

Step5. Signature verification

Recipient B does the following:-

1. Uses sender A's public key (n, e) to compute integer $v = s^e \bmod n$.
2. Extracts the message digest from this integer.
3. Independently computes the message digest of the information that has been signed.
4. If both message digests are identical, the signature is valid.

8. Conclusions

Among the many IT giants driven by trends in cloud computing has not doubtful. It gives almost everyone has brought good news. For enterprises, cloud computing is worthy of consideration and try to build business systems as a way for businesses in this way can undoubtedly bring about lower costs, higher profits and more choice; for large scale industry, After the financial turmoil will be the cost of infrastructure for large-scale compression seems likely; developers, when in the face of cloud computing, through the PaaS model can effectively improve their own capacity, Therefore, the impact of cloud computing on the ISV is the largest of the many roles; for engineers and developers are concerned. There is the advent of cloud computing is bound to birth a number of new jobs. The clouds will grow in size as soon as available bandwidth and the corresponding service model mature enough, cloud computing will bring a revolutionary change in the Internet. Cloud computing announced a low-cost super-computing services to provide the possibility, while there are a large number of manufacturers behind, there is no doubt that cloud computing has a bright future.

References

[1]http://en.wikipedia.org/wiki/Cloud_computing

[2]http://www.cloudcomputingchina.cn/Article/luilan/200909/306.html

[3]http://searchcloudcomputing.techtarget.com/sDefinition/0, sid201_gci1287881,00.html

[4]http://www.boingboing.net/2009/09/02/cloud-computing-skep.html

[5] (U.S.) Nicholas. Carr, fresh Yan Yu, "IT is no longer important: the Internet great change of the high ground - cloud computing," The Big Switch:Rewining the World,from Edison to Google, , CITIC Publishing House, October 2008 1-1

[6] Ya-Qin Zhang, the future of computing in the "cloud - Client", The Economic Observer reported, http://www.sina.com.cn, 2008 Nian 07 Yue 12 Ri 14:30

[7] Wang Haopeng (Air Force Aviation University of Computer Teaching, Jilin, Changchun 130022, China); Liu strong (Air Force Air University, Research Department, Jilin, Changchun 130022, China), virtualization technology in the application of cloud computing, TP313.A ,1009-3044 (2008) 25-1554-01,2008 Year 25

[8] http://www.emc.com/digital_universe