Security issues in Cloud Computing

Kalyani D. Kadam
Faculty of Computer Science in Symbiosis International University, Pune

Sonia K. Gajre
Faculty of Computer Science in Symbiosis International University, Pune

R. L. Paikrao
Faculty of engineering in Amrutvahini College of Engineering, Sangamner

ABSTRACT
It is very important to take security and privacy into account when designing and using cloud services. In this paper security in cloud computing was elaborated in a way that covers security issues/concerns and challenges , security standards and security management models and Digital Signature with RSA encryption algorithm to enhance Data Security in Cloud .
–Security issues/concerns indicate potential problems which might arise.
–Security standards offer some kind of security templates which cloud service providers (CSP) could obey. The most promising standard for the future would be OVF format which promises creation of new business models that will allow companies to sell a single product on premises, on demand, or in a hybrid deployment model.
–Security management models offer recommendations based on security Standards best practices
–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.

1. INTRODUCTION
A cloud computing framework, paired with technologies such as netbooks, rich internet applications (RIA) s, smart phones, and web services, allows users to run their applications anywhere and access services at any time.

Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid. While it is sometimes considered simply an alternative means of traditional server or website hosting, the Cloud is actually much more than that, offering many different layers and opportunities. Of particular benefit is the flexible infrastructural platform that Cloud computing provides, which can change computing resources from a Capital- and skill-intensive investment into an elastic-scale utility-model of allocation.

Cloud computing is clearly one of today's most enticing technology areas due, at least in part, to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model.

2. SECURITY IN THE CLOUD
Today, enterprises are looking toward cloud computing horizons to expand their on-premises infrastructure, but most cannot afford the risk of compromising the security of their applications and data. Security ranked first as the greatest challenge or issue of cloud computing .Security and privacy affect the entire cloud computing stack, since there is a massive use of third-party services and infrastructures that are used to host important data or to perform critical operations

Corporations and individuals are concerned about how security and compliance integrity can be maintained in this new environment

As cloud computing encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management ,there are numerous security issues for cloud computing. Therefore, security issues for many of these systems and technologies are applicable to cloud computing.

For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns.

2.1 Security Concerns/Issues
1) Security concern #1: With the cloud model control physical security is lost.
2) Security concern #2*:* Company has violated the law (risk of data capture by (foreign) government).
3) Security concern #3: Service incompatibility
4)Securityconcern#4*:* Who controls the encryption/ decryption keys? Logically it should be the customer.
5) Security concern #5: Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exist.
6) Security concern #6: Users must keep up to date with application improvements to be sure they are protected.
7) Security concern #7: Some government regulations have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customer's financial data remain in their home country.
8) Security concern #8: The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the auditability of records.
9) Security concern #9: Customers may be able to sue cloud service providers if their privacy rights are violated. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties

2.2 Security management standards

Security standards offer some kind of security templates which cloud service providers (CSP) could obey.

1. Information Technology Infrastructure Library (ITIL),
2. ISO/IEC 27001/27002
3. Open Virtualization Format (OVF).

1. Information Technology Infrastructure Library (ITIL),

It is set of best practices and guidelines that define an integrated, process-based approach for managing information technology services.

ITIL breaks information security down into:

- Policies: The overall objectives an organization is attempting to achieve
- Processes: What has to happen to achieve the objectives?
- Procedures: Who does what and when to achieve the objectives?
-Work instructions: Instructions for taking specific actions

A basic goal of security management is to ensure adequate information security. The primary goal of information security, in turn, is to protect information assets against risks, and thus to maintain their value to the organization. This is commonly expressed in terms of ensuring their confidentiality, integrity and availability along with related properties or goals such as authenticity, accountability and reliability

2. ISO/IEC 27001/27002

ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). It is also a certification standard and uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS.

Essentially, the ITIL ISO/IEC 20000, and ISO/IEC27001/27002 frameworks help IT organizations internalize and res pond to basic questions such as:

-"How do I ens ure that the current security levels are appropriate for your needs? "

-"How do I apply a security baseline throughout your operation? "

3. Open Virtualization Format (OVF).

OVF enables efficient flexible and secure distribution of enterprise software, facilitating the mobility of virtual machines and giving customers vendor and platform independence. Customers can deploy an OVF formatted virtual machine on the virtualization platform of their choice.

With OVF, customer's experience with virtualization is greatly enhanced, with more portability, platform independence, verification, signing, versioning, and licensing terms. OVF lets you:

- Improve your user experience with streamlined installations
- Offer customers virtualization platform independence and flexibility
- Create complex pre-configured multi-tiered services more easily
- Efficiently deliver enterprise software through portable virtual machines
- Offer platform-specific enhancements and easier adoption of advances in virtualization through extensibility

And because a virtual appliance is simply a file with a wrapper (the XML description), it's easy to replicate and distribute such appliances with all security and privacy configurations.

In the future, clouds that are enabled by a virtualization layer will provide new go-to-market opportunities, and software appliances (software products that integrate operating system and layered software into an easily managed composite package that can be deployed aboard industry-standard client or server hardware, either on a virtual machine or directly on the hardware) will help simplify this transition.

2.3 Security management models

This section describes twenty recommended security management models and their requirements for cloud computing that cloud service providers should definitely consider as they develop or refine their compliance programs.

2.3.1 Software-as-a-service(saas) security: -

SaaS is the dominant cloud service model for the foreseeable future and the area where the most critical need for security practices and oversight will reside.

–Privileged user access: Get as much information as you can about the people who manage your data. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

–Regulatory compliance: Make sure that the vendor is willing to undergo external audits and/or security certifications.

–Data location: Ask providers if they will commit to storing and processing data in specific juries dictions , and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers .

–Data segregation: Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

–Recovery: Even if you don't know where your data is ,a cloud provider should tell you what will happen to your data and service in case of a disaster

–Investigative support: Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co -located and may also be spread across an ever-changing set of hosts and data centers .

–Long-term viability: Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company

To address the security issues listed above, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolve.

2.3.2 Security management (people):

One of the most important actions for a security team is to develop a formal charter for the security organization and program. The charter should be aligned with the strategic plan of the organization or company the security team works for

2.3.3 Security governance:

A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies. This committee must clearly define the roles and responsibilities of the security team and other groups involved in performing information security functions.

2.3.4 Risk management and assessment:

Risk management entails identification of technology as identification of data and its links to business s processes, applications, and data stores; and assignment of ownership and custodial res possibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls. Security risk assessment is critical to helping the information

security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets.

2.3.5 Security awareness:

People are the weakest link for security. Knowledge and culture are among the few effective tools to manage risks related to people. Not providing proper awareness and training to the people who may need them can expos e the company to a variety of security risks for which people, rather than system or application vulnerabilities, are the threats and points of entry.

2.3.6 Education and training:

Programs should be developed that provide a baseline for providing fundamental security and risk management skills and knowledge to the security team and their internal partners.

2.3.7 Policies and standards:

Many resources and templates are available to aid in the development of information security policies and standards.

2.3.8 Third party risk management:

Lack of a third-party risk management program may result in damage to the provider's reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third- party vendors.

2.3.9 Vulnerability assessment:

Classifies network assets to more efficiently prioritize vulnerability-mitigation programs, such as patching and system upgrading.

2.3.10 Security image testing:

Virtualization-based cloud computing provides the ability to create "Test image" VM secure builds and to clone multiple copies. Gold image VMs also provide the ability to keep security up to date and reduce exposure by patching offline.

2.3.11 Data governance:

This framework should describe who can take what actions with what information, and when, under what circumstances and using what models.

2.3.12 Data security:

Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the European Union. It can also force encryption of certain types of data, and permit only specific users to access the data. It can provide compliance with the Payment Card Industry Data Security Standard (PCIDSS).

2.3.13 Virtual machine security:

In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers..

2.3.14 Physical security:

Since customers lose control over physical assets, security model may need to be reevaluated. The massive investment required to build the level of security required for physical data center is the prime reason that companies don't build their own data centers, and one of several reasons why they are moving to cloud services in the first place. Some samples of controls mechanisms:

- 24/7/365 onsite security.
- Biometric hand geometry readers.
- Security cameras should monitor activity throughout the facility.
- Heat, temperature, air flow, and humidity should all be kept within optimum ranges for the computer equipment.
- Policies, processes, and procedures are critical elements of successful physical

Security that can protect the equipment and data housed in the hosting center.

3. 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. 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.

3.1. RSA algorithm

RSA was created by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. The RSA scheme is a block cipher in which the plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 21024.

Till now, it is the only asymmetric (i.e. needs two different keys) algorithm used for private/public key generation and encryption.RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations.

The RSA algorithm involves three steps

- Key generation
- Encryption
- Decryption

Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Figure 3.1.1 The RSA Algorithm

3.2. 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 3.2.1)

Figure 3.2.1 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)

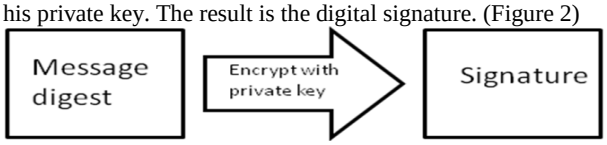
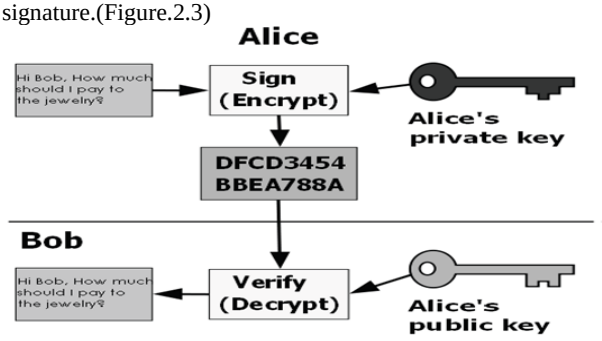


Figure 3.2.2 Encryption of message digest into Signature

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.2.3)



Fiure 3.2.3.Encryption of Digital Signature into Cipher text

3.3.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.

Step1. 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 × 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.

4. ACKNOWLEDMENTS

Our thanks to Prof.Shraddha Phansalkar, Prof. Ambika V.Pawar and Prof Swati Ahirrao for their valuable support.

5. REFERENCES

[1] Uma Somani, Kanika Lakhani and Manish Mundra **"Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing"**, 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[2] Kresimir Popovic and Zeljko Hocenski **"Cloud computing security issues and challenges"**, MIPRO 2010, May 24-28, 2010, Opatija, Croatia.

[3] Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina **"Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control"**, CCSW'09, November 13, 2009, Chicago, Illinois, USA

[4] Cloud Security Alliance **"Top Threats to Cloud Computing"**

[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] S. Pearson, **"Taking Account of Privacy when Designing Cloud Computing Services"**, CLOUD'09, May 23, 2009, Vancouver, Canada

[7] M. Casassa-Mont, S. Pearson and P. Bramhall, **"Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services",** Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382

[8] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,

http://www.cloudsecurityalliance.org/, December 2009

[9] http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def- v15.doc