International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Analysis of Cloud Security Issues and Security Architecture Based on RSA, Tokenization and Digital Signature

Niharika[Á] and Deepak Rastogi[Á*]

[Á]Department of Computer Science, Dr. K. N. Modi University, Newai,Rajasthan, India

Accepted 10 May 2014, Available online 01 June 2014, **Vol.4, No.3 (June 2014)**

Abstract

Cloud computing is a shift from physical to network paradigm using the concept of virtualization, utility computing, distributed network and resource sharing. Cloud may be a major step in the science and technical environment but it comes with an added level of risk due to handling over of our data and resources to the network under the cloud platform. In order to maintain the privacy and integrity of data, the data must be cryptographically secure and also the user virtual machine should be physically isolated while migration. In this paper we identify major security issues in cloud and their solutions. In addition we propose the implementation of an encryption architecture based on the very secure RSA algorithm, tokenization and digital signature.

Keywords: *Cloud architecture, Service Models, RSA, Tokenization, Digital Signature*

1. Introduction

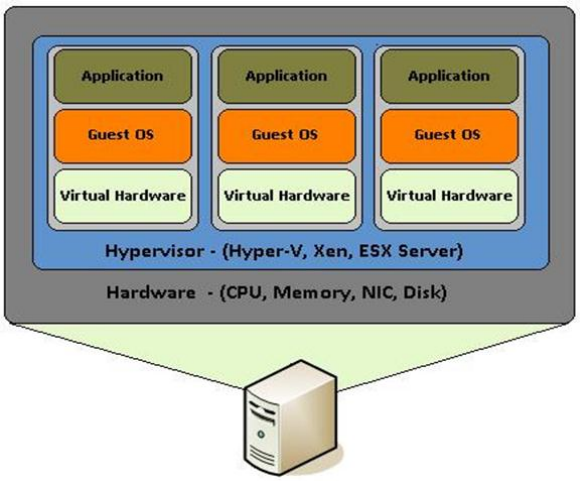
Cloud computing, the new technological advancement is an information system architecture which has caught the attention of all the leading companies of the world. Cloud computing is a model for enabling convenient, on-demand network access, to a shared pool of configurable computing resources, (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Chittaranjan Hota *et al*,2011).This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud computing is a shift from physical to network paradigm, here all the processes are similar except that the platform is changed here, hence large storage space, less expensive, less manual work through resource sharing, distributed computing and utility computing.It allows users to use various applications without the installation or updation of the software or hardware. Cloud provides on demand services based on utility computing such a software, infrastructure, platform and database through the internet. Cloud leverages the users from the heavy burden of software and hardware installations which generally occupies large space in our system and also is time consuming and the pay-as-per-usage system is very cost effective.82% of the companies have reportedly saved money by moving to the cloud and 80% of cloud adopters saw improvements within 6 months of moving to the cloud . The basis of cloud computing is virtualization which makes sharing of resources, connectivity amongst users at any corner of the world easier. So if cloud computing is such a boon to the scientific and industrial communities then why is it that many IT companies are reluctant in implementing cloud. Everything comes with a price and so does cloud. The entire cloud paradigm lies over the internet, hence the user's data and resources are distributed across various cloud servers so the data stored in a cloud server is exposed to cyber theft. In this paper we highlight the various ongoing as well as emerging cloud security issues, their solutions and the future of cloud computing ,we also discuss , is cloud computing really worth all the risk and will the leading IT brains be able to make a security-issue free infrastructure for cloud computing.

There are four types of cloud computing models listed by NIST (2009): private cloud, public cloud, hybrid cloud and community cloud.

1. **Public Cloud**: In a public cloud the resources, applications and services over the internet provided by any public organization can be accessed by the general public. The services may be free or may cost the user as per the user's usage, depending on the resource. Example: EC2,IBM Blue Cloud, Sun Cloud, Google App Engine and Windows azure service platform(Pankaj Arora *et al*,2012).
2. **Private cloud**: A private cloud is privately owned and managed by an organization within a firewall. The private cloud model is adapted by those IT companies which need high level of data security. Basically a private cloud is a datacenter having its own set of virtual machine where data is managed and shared without any security issues since private cloud comes with very high security. Generally in a cloud implemented organizations the users need to wait for the IT resources to be free which can take weeks, this

*Corresponding author: **Deepak Rastogi**

can further lead to bottlenecks, piling up of workloads. A private cloud overcomes this drawback by providing immediate shared resources to the developers. Hence this reduces time and management tasks .The developers can focus on projects rather than on time consuming tasks. The high level of performance and software quality is maintained until and unless the cloud is free of any authorized malicious user. One major drawback is that it is expensive. Examples of community cloud include Google's "Gov Cloud"(Dimitrios Zissis,2012).



3. **Hybrid Cloud**: If the cloud model utilizes the concept of public, private and community cloud then such a model is called as a hybrid cloud. This model is generally used by large organizations such as IBM where public services need to be provided, security of their data needs to be kept confidential, various data centers need to be managed. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities (Pankaj Arora *et al*,2012).
4. **Community Cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise. Its cost is lesser then public cloud but more than private cloud.

2. Virtualization

Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others. It allows abstraction and isolation of lower-level functionalities and underlying hardware. This enables portability of higher-level functions and sharing and/or aggregation of the physical resources (Nariman Mirzaei,2008).Through virtualization user can create virtual machines and use them as per requirement such as migration, sharing and roll back. Virtualization makes resource sharing easier. Cloud service providers (CSP) provide IaaS, which is an environment for creating virtual machines and various other functions such as migration.

Through virtualization we can install more than one guest operating system on a single host operating system providing each operating system its own isolated environment as if it were the only one utilizing the hardware resources .These guest operating systems are also known as virtual machines (VM).Hence we can run numerous applications in our system which would not have been compatible in our host operating system. But virtualization comes with a heavy software as well as heavy cost besides virtualized environments are vulnerable to all types of attacks for normal infrastructures; VMwatcher, VMwall were developed to monitor the VMs from outside the VM but this could only monitor over certain features such as memory pages, disk blocks and low level instructions. So X-SPY,LARES and VMsec were developed which monitor from inside the VM.however, security is agreater challenge as virtualization adds more points ofentry and more interconnection complexity [read3]. Cloud utilizes the concept of virtualization so this is where the major security issues emerge from. In order to completely utilize the benefits of cloud computing we need to work with virtualized systems which includes techniques such as migration, copying and roll back. In a normal physical system with virtual machinesall the VMs are controlled by a hypervisor.

2.1 Hypervisor

Hypervisor manages all the virtual machines in a system. A hypervisor is a program that would enable you to host several different virtual machines on a single hardware. Each one of these virtual machines or operating systems you have will be able to run its own programs, as it will appear that the system has the host hardware's processor, memory and resources. In reality, however, it is actually the hypervisor that is allocating those resources to the virtual machines. The hypervisor loads the client operating systems of the virtual machines. The hypervisor allocates the correct CPU resources, memory, bandwidth and disk storage space for each virtual machine.

Hypervisor acts as an abstraction layer which provides the necessary resource management functions that enable the sharing of hardware resources between vms (Amani S Ibrahim *et al*,2010). It can access all physical devices residing on a server. It can also access the memory and disk. It can control all aspects and parts of a virtual machine. In effect, a hypervisor allows you to have several virtual machines all working optimally on a single piece of computer hardware.

Hypervisor Issues: But hypervisor is the most vulnerable software in the virtualization layer since it has information regarding resources of all the virtual machines so it has been the prime target of all the hackers. A hypervisor is vulnerable to a lot of malicious code, especially those

coming from a rogue virtual machine; almost 35% of vulnerabilities found in server virtualization were related to the hypervisor. Hypervisors are attacked by VM-Based rootkits.Providers such as Microsoft and VMware have also been working to make their hypervisors more secure. HyperJacking ,BLUEPILL, Vitriol , SubVirand DKSM are well-known attacks that target thevirtual layer at run-time(Amani S Ibrahim *et al*,2010). An attacker can compromise the migration module in the hypervisor and transfer a victim virtual machine to a maliciousserver. Also, it is clear that VM migration exposes thecontent of the VM to the network, which can compromiseits data integrity and confidentiality. A malicious virtualmachine can be migrated to another host (with another hypervisor) compromising it.

2.2 Shared Resources

VMs located on the same server can share CPU, memory,I/O, and others. Sharing resources between VMs may decrease the securities of each VM. For example, a malicious VM can infer some information about other VMs throughshared memory or other shared resources without need of compromising the hypervisor. Using covert channels, two VMs can communicate bypassing all the rulesdefined by the security module of the VMM. Thus, a malicious Virtual Machine can monitor sharedresources without being noticed by its VMM, so theattacker can infer some information about other virtual machine(David G Rasoda *et al*,2013).

2.3 VM Image

When there is a need to create various virtual machines which have similar set up procedure then an image is captured of an already configured virtual machine which acts as a template for the setup of rest all the similar VMs. Hence an image is a virtual hard disk file or a prepackaged software template. Amazon offers a public image repository where legitimate users can download or upload a VM image (David G Rasoda *et al*,2013).

VM Image Issue: The issue with a virtual image is that it can be altered by a valid malicious user and when other customers use it to create a virtual machine, the VM created will be infected. Data leakage can also take place supposing, while creating an image confidential data such as username and passwords or keys are also recorded. Hence it is important to check whether the image is containing any private data before making the image public or before providing it to other customers.

2.31 Virtual machine rollback

Virtual machines are able to be rolled back to their previous states if an error happens. But rolling back virtual machines can re-expose them to security vulnerabilities that were patched or re-enable previously disabled accounts or passwords. In order to provide rollbacks, we need to make a “copy” (snapshot) of the virtual machine, which can result in the propagation of configuration errors and other vulnerabilities(David G Rasoda *et al*,2013).

3. Cloud Service Models

Cloud service models are commonly divided into SaaS, PaaS, and IaaS.

3.1 SaaS

Software as a service or software on demand is the simplest of all the three models since it provides maximum abstraction at the user level, the complex cloud infrastructure is kept hidden from the user. SaaS provides on demand applications or software to the customers based on utility computing from various client devices through thin client interface, such as a web browser (e.g. web-based e-mail).The consumer does not manage orcontrol the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. The security of data is least in this model since the user loses control over data the moment data enters the internet field the users data can be stored in any cloud server at any part of the world. Moreover since the user has no idea of the infrastructure the security of the data is unknown. But SaaS is very cost effective since it leverages the user from the heavy burden of installing the software which would consume storage space in our system and the duty of maintaining the software and updating is the responsibility of the service provider. Eg: Sales force, Google Mail, Google Docs.

3.2 PaaS

Platform-as-a-service model provides the customer a platform where applications can be developed and tested and also users can run existing applications by renting virtualized server and its related services. The user has control over the applications and the application hosting environment configuration. PaaS offers a platform to build and deploy SaaS applications. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts. On the downside, PaaS involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform (Pankaj Arora *et al*,2012).since the user is responsible for developing the application hence the developer duty to keep the developing environment

Table 1 Difference between the three service models.

SaaS	PaaS	IaaS
End client applies to a person or organization who subscribes to a service offered by a cloud provider and is accountable for its use. (Dimitrios Zissis,2012). Client has absolutely no control over the data.	Developer–moderator applies to a person or organization that deploys software on a cloud infrastructure. (Dimitrios Zissis,2012). Client has no access to the underlying layer except for the design of application; hence major security is under the hands of the CSP.	Owner applies to a person or organization that owns the infrastructure upon which clouds are deployed (Dimitrios Zissis,2012). Data security responsibility equally shared by client and provider.
Clients have no control over the performance level of the application.	Developers always need to worry about the frequent updation of their application to cope up with the changing market developer has control only over the upper layers.	The complete infrastructure is in the hands of the developer.it depends on the developer how to create the application in what type of network background and what server to use.
The risk of data leakage is very high.	The risk of data leakage is high but not as high as compared to SaaS.	The risk is reduced here since the client owns the major control over all the layers.
It works in the application level.	It works in the virtual level.	It works in the physical level.
Systemrequirements: • Privacy in multitenant Environment • Data protection from exposure (remnants) • Access control • Communication protection • Software security • Service availability	• Access control • Application security • Data security, (data in transit, data at rest, remanence) • Software interruption (deletion) • Cloud management control security • Impersonation • Secure images • Virtual cloud protection • Communication security	• Legal not abusive use of cloud computing • Hardware security • Hardware reliability • Network protection •Network resources protection
Threats:- • Interception • Modification of data at restand in transit • Data interruption (deletion) • Privacy breach • Impersonation • Session hijacking • Traffic flow analysis • Exposure in network	• Programming flaws • Software interruption • Software modification • Software interruption (deletion) • Cloud management control security • Impersonation • Session hijacking • Traffic flow analysis • Exposure in network • Defacement • Connection flooding • DDOS • Impersonation	• Network attacks • Connection flooding • DDOS • Hardware interruption • Hardware theft • Hardware modification • Misuse of infrastructure • Natural disasters

flexible enough to cope up with the fast changing market hence frequent updation is required. The developer has control only over the application not on the infrastructure over which the application is deployed.so the user cannot completely trust the infrastructure environment. Eg: Google App Engine, windows azure.

3.3 IaaS

It is a provision model in which Provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources, and allow the consumer to deploy and run arbitrary software, which can include operating systems and applications. The consumer has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (Dimitrios Zissis,2012).In this model users have maximum control over their data security since the complete infrastructure is provided in which the users can deploy their cloud but the control over the network is in the hands of the service provider. Hence there is a minimum chance of data leakage until and unless there is a loop hole in the hypervisor. Eg amazon EC2.Even IaaS is not completely secure it also has various security issues. The table 1 illustrates the differences between the three service models.

4. Cloud Data Security

The very moment we use cloud applications to store our data, we lose control over data. The data in cloud can be stored at any location in the globe. Generally the data protection law is based on the premise that it is always clear where personal data is located, by whom it is processed and who is responsible for data processing. But cloud computing seems to violate this law since the customers are clueless regarding their data location or what keys are being used to protect their data over the internet in cloud. Globally, 47% of those who are currently using a cloud computing service reported they have experienced a data security lapse or issue with the cloud service their company is using within the last 12 months. India had the highest incidence (67%), followed by Brazil (55%). Incidence of data security lapse or issue increased from 43% in 2011 to 46% (excluding Brazil, which was not surveyed in 2011) in 2012. India had the biggest increase of 12%, followed by Japan (7% increase) and Canada (6% increase).

Cloud computing may be the most trending and first among the top ten most important technologies but it has a lot of loop holes. In this topic we shall discuss about these loop holes and what measures have been taken to overcome them to so that cloud can have a better prospect in the future successive years.

Cloud computing has two components, USER and PROVIDER. The cloud service provider provides online services such as application, storage ,infrastructure ,resources to the customer and the customer utilizes these resources on basis of pay as per usage. There can be a malicious user or a provider so security issues can rise from both the components. So rectification techniques and data security laws need to be developed for both user as well as provider. Rectification techniques can be applied by using cryptography but this is not enough to prevent data from hackers hence physical isolation of the data in a system from other machines in cloud successfully helps in creating a secure cloud.

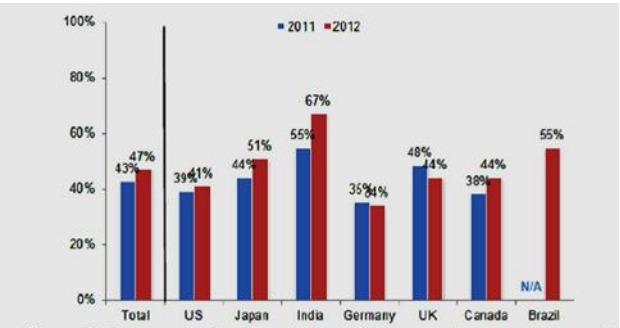


Figure 7: Data security lapse statics in different countries around the world

Figure 3: Cloud security attacks

Cloud Security Issues

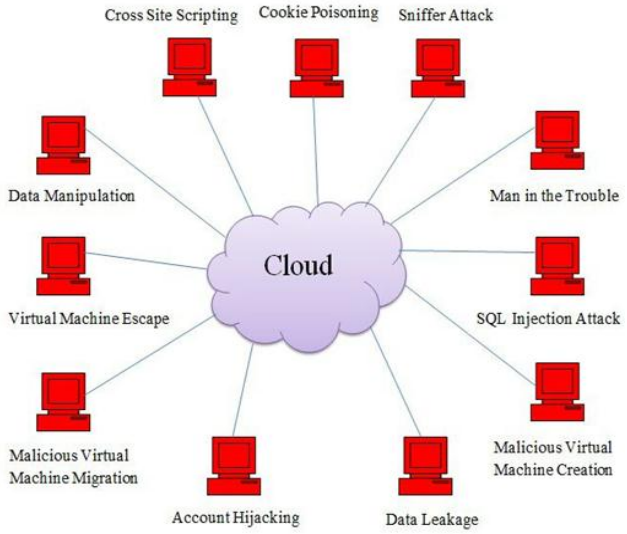
Issues and Solutions Regarding Physical Isolation

4.1 Virtual Machine Escape

It is designed to exploit the hypervisor in order to take control of the underlying infrastructure. In this attack the hacker seeks control over the host operating system and all the virtual machines by running malicious code in the VM.

Rectification measures

4.1.1 Hypersafe



For malware to affect a hypervisor, it typically needs to run its own code in the hypervisor. HyperSafe utilizes two components to prevent that from happening. First, the HyperSafe program has a technique called non-bypassable memory lockdown, which explicitly and reliably bars the introduction of new code by anyone other than the hypervisor administrator. This also prevents attempts to modify existing hypervisor code by external users. Second, HyperSafe uses a technique called restricted pointer indexing. This technique initially characterizes a hypervisor's normal behavior, and then prevents any deviation from that profile. Only the hypervisor administrators themselves can introduce changes to the hypervisor code. Hence hypersafe ensures the hypervisor isolation and prevents it from attacks such as modification of the hypervisor code, execution of the injected code, modification of the page table, and tamper from a return table.

4.1.2 Trusted Cloud Computing Platform

TCCP enables providers to offer closed box execution environments, and allows users to determine if the environmentis secure before launching their VMs. The TCCPadds two fundamental elements: a trusted virtual machinemonitor (TVMM) and a trusted coordinator (TC). TheTC manages a set of trusted nodes that run TVMMs, andit is maintained but a trusted third party. The TC participates in the process of launching or migrating a VM, which verifies that a VM is running in a trusted platform. TCCP has a significantdownside due to the fact that all the transactions have toverify with the TC which creates an overload. They proposedto use Direct

Anonymous Attestation (DAA) and Privacy CA scheme to tackle this issue(David G Rasoda *et al*,2012).

4.1.3 Private Virtual Infrastructure

A datacenter is in itself is a complete system with its own set of VMs. But interaction of the datacenter with cloud corrupts the center due to various malicious users in cloud. PVI provides isolation to datacenter. Interaction within PVI is done via Virtual Private Networking and encryption with IPSec or SSL tunnels. Cloud security service reports are cryptographically bound and signed. IBM's Trusted Virtual Datacenter (TVDc) provides many features in Cloud Computing environment for proper security of Datacenter Servers and VM isolation through secure Hypervisor called sHype which when coupled with TCG-based property verification (IMA) provides strong levels of containment and trust.Fabric pre-measurement is what allows PVI to share the responsibility of security management between the service provider and client. Pre-measurement is performed by a LoBot, which tests the fabric's security posture before provisioning occurs, allowing the information owner to determine the safeness of the fabric before deployment of aPVI.

4.2 Malicious Vm Migration

Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can access data illegally during migration, transfer a VM to an untrusted host, create and migrate several VM causing disruptions or DoS.

Rectification Measures

4.2.1 PALM

PALM proposes a secure live migration framework that preserves integrity and privacy protection during and after migration. The prototype of the system was implemented based on Xen and GNU Linux, and the results of the evaluation showed that this scheme only adds slight downtime and migration time due to encryption and decryption.

4.2.2 VNSS

VNSS proposes a security framework that customizes security policies for each virtual machine, and it provides continuous protection thorough virtual machine live migration. They implemented a prototype system based on Xen hypervisors using stateful firewall technologies and user space tools such as iptables, xmcommands program and conntrack-tools. The authors conducted some experiments to evaluate their framework, and the results revealed that the security policies are in place throughout live migration.

4.3 Account Hijacking

In mobile cloud computing the user account is protected by a username and password and it is not an impossible task to a hack a user account. So how could the system confirm that the user logging in is the account is the actual user?

Rectification Measures

4.3.1 Enhanced Dynamic Credentials

The proposed scheme offloads the frequently occurring dynamic credential generation operations on a trusted entity to keep minimum processing burden on the mobile device. To enhance the security and reliability of the scheme, the credential information is updated frequently on the basis of mobile-cloud packets exchange. Furthermore, the proposed scheme is compared with the existing scheme on the basis of performance metrics i.e. turnaround time and energy consumption.

4.4 Malicious Virtual Machine Creation

Insertion of malicious code in virtual image can lead to creation of malicious virtual image and when hosted on servers or datacenters, these machines can cause significant damage.

Rectification Measures

4.4.1 Mirage

Through mirage one can create a secure network application or software on the cloud platform.Code can be developed on a normal OS such as Linux or MacOS X, and then compiled into a fully-standalone, specialized kernel that runs under the hypervisor. Mirage uses the OCaml language, with libraries that provide networking, storage and concurrency support that work under UNIX during development, but become operating system drivers when being compiled for production deployment. The framework is fully event-driven, with no support for preemptive threading.One limitation of this approach is that filters may not be able to scan all malware or remove all the sensitivedata from the images. Also, running these filtersmay raise privacy concerns because they have access tothe content of the images which can contain customer's confidential data. Mirage 1.0 has been released recently.

4.5 SQL Injection Attacks

SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it. For example an argument value of variable y or 1==1 may cause the return of full table because 1==1 is always seems to be true.[9]

4.6 Cross Site Scripting (Xss) Attacks

Various techniques like: Active Content Filtering, Content

Based Data Leakage Prevention Technology, Web Application Vulnerability Detection Technology has already been proposed to prevent XSS attacks. These technologies adopt various methodologies to detect security flaws and fix them. A blueprint based approach that minimizes the dependency on web browsers towards identifying untrusted content over the network has been proposed in.

4.7 Man in the Middle Attacks (MITM)

This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured. For example if two parties are communicating with each other and SSL is not properly installed then all the data communication between two parties could be hack by the middle party. Counter measure for this attack is SSL should properly install and it should check before communication with other authorized parties.

4.8 DNS Attacks

Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some malicious connection.

4.9 Sniffer Attacks

Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network for example an attacker can hack passwords that are not properly encrypted during communication. If the communication parties not used encryption techniques for data security then attacker can capture the data during transmission as a third party. Counter measure for this attack is parties should used encryption methods for securing there data(Sara Qaisar *et al*,2012).

4.2.8 Cookie Poisoning

This can be avoided either by performing regular cookie cleanup or implementing an encryption scheme for the cookie data. This can be achieved by the scheme introduced in. The introduced scheme seems to act reasonably in confronting cookie poisoning attack.

5. Issues and Solutions using the Concept of Cryptography

5.1.1 Data Leakage

In cloud environment data may be stored at any location in the globe. Data security and access control is one of the most challenging ongoing research work in cloud computing, because of users outsourcing their sensitive data to cloud providers. Existing solutions that use pure cryptographic techniques to mitigate these security and access control problems suffer from heavy computational overhead on the data owner as well as the cloud service provider for key distribution and management**.** Physical isolation alone cannot serve as a strong tool against unauthorized access, even if hackers get to access the data somehow, the data must be properly encrypted such that the hacker will not be able to decrypt the data.

Rectification Measures

5.1.1 Digital Signature

Digital signatures enable the "authentication" and ―non-repudiation‖ of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

5.1.2 Fragmantation Redundancy Scattering

This technique consists in first breaking down sensitive data into insignificant fragments, so any fragment does not have any significant information by itself. Then, fragments are scattered in a redundant fashion across different sites of the distributed system(David G Rasoda *et al*,2012).

5.1.3 Homomorphic Encryption

In homomorphic encryption, the data while in the network never gets decrypted. The operations are done on the encrypted data itself and the encrypted data is sent to the user. The solution when decrypted gives the original data. Hence in this technique data is never exposed in the network. IBM's HE has not yet been implemented but it could revolutionize security.

5.1.4 Encryption Algorithm

Encrypting data increases the security of data, but only encryption is just not enough to guarantee secure data. The algorithms that is chosen for encryption and the complexity of the encryption has a major say in whether the data will be able to main its privacy and integrity.

RSA Algorithm: RSA algorithm was proposed by Rivest, Shamir and Adleman of MIT in 1977.

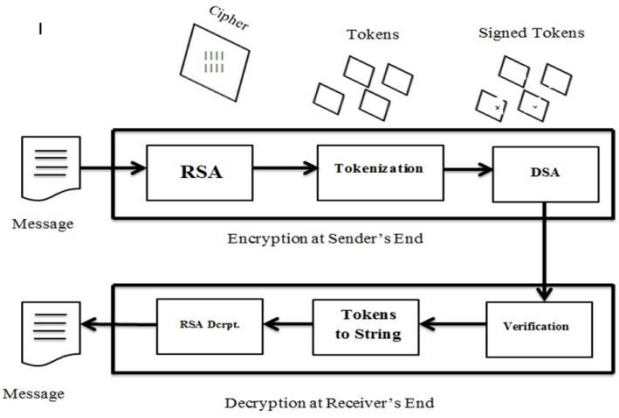


Figure 4: Encryption Architecture

RSA is based on exponentiation in a finite (Galois) field over integers modulo a prime. The exponentiation takes $O((\log n)^3)$ operations. It uses large integers (eg. 1024). The security is due to cost of factoring large numbers. The factorization takes $O(e^{\log n \log \log n})$ operations. In RSA, each user generates a key pair (public and private key) by selecting two large primes at random (p, q) and computes their modulus.

N=p.q

By selecting, at random the encryption key e (where $1<e<\phi(N)$, $\gcd(e,\phi(N))=1$) solve the following equation to find decryption key d.

$e.d=1 \bmod \phi(N)$ and $0 \le d \le N$

Each user publish their public encryption key like,

PU={e,N}

And private key is kept secret for decryption.

PV={d,p,q}

$C=M^e \bmod N$, where $0 \le M < N$

To encrypt a message M, the sender obtains **public key** of recipient PU={e,N} and computes:

String Tokenization

The cipher generated through the RSA algorithm goes through the next phase of our algorithm ie tokenization. Tokenization is a process of replacing sensitive data with a surrogate value (called token), which are randomly selected values. In this process data size is reduced. To tokenize our encrypted data, we will use the following function (F): from equation (1),

$F::parse(C,d,t_1,t_2,t_3\ldots)$ (2)

Where,

t_i = Token value; where i= number of token

C= Encrypted message through RSA

d = delimeter (characters that separate the tokens)

Generating digital signature

The process receives a set of tokens as input so that a loop will be required upto the number of tokens. Digital signature for data can be generated using the private key and to export the public key and the signature to files.

There are three parameters that can be common to a group of users. These are:

1. A 160-bit prime number q is chosen.
2. A prime number p with length between 512 and 1024-bits such that q divides (p-1).
3. g is chosen to be of the form $h^{(p-1)/q} \bmod p$,
4. where, h is an integer between 1 and (p-1); $g>1$[2]

With these numbers in hand, users select a private key and generates its corresponding public key. The private key should be a number from 1 to (q-1) which should be chosen randomly. The public key is calculated as:

$y=g^x \bmod p$

where,

y is public key, and

x is private key.

To create a signature, user calculates two functions r and s which are functions of public key components (p,q,g), the user's private key (x), the hash code of the message H(T), an additional integer k should be generated randomly.

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1} (H(T)+xr)] \bmod q$

Signature=(r,s)

Verification

At the receiving end, verification is performed using formulas:

$w= (s')^{-1} \bmod q$

$u_1= [H(T')w] \bmod q$

$u_2= (r')w \bmod q$

$v= [(g^{u1} y^{u2}) \bmod p] \bmod q$

Test: v=r'

Where,

M= Tokens to be signed

H(T)= hash of T using SHA-1

T',r',s' = received versions of T,r,s

Converting Tokens to String

After verifying the signature, receiver will get the set of tokens (or substrings of the main message).To convert the tokens into string, we are required the set of tokens along with the delimeter which will convert the number of tokens (or substrings) into a single string. Hence the receiver will find out the cipher text.

RSA Decryption

To decrypt the cipher text (C) the receiver uses his private key PV={d,p,q} and computes:

$M=C^d \bmod N$

6. **Security Issues Related to Provider**

Here are six of the specific security issues that customers should raise with vendors before selecting a cloud vendor.

1. **Privileged user access**. Users should collect as much information as possible about the people who manage data.SLA agreement provides a set of rules that both the provider and user needs to follow. User should go through the agreements carefully.

2. **Regulatory compliance**. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications.

3. Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. user should Ask providers if they will commit to store and

process data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4. Data segregation. User should have knowledge of the encryption techniques used by service providers to secure their data.

5. 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. User should know if in case of any error occurrence how to recover their data.

6. 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. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible.

Conclusion

In this paper we have analyzed various cloud security issues both on the user as well as on the provider side and various solutions that are developed to overcome these problems. Hence we conclude that if a security mechanism is developed it should provide physical isolation to the data and also should be cryptographically secure. Cloud may have various negative aspects regarding data security but cloud has certainly changed the way we communicate over the internet. Promising security techniques have already been developed and research is going on, on certain techniques such as Homomorphic encryption which will revolutionize security to a new level. In the next 5 years, a 44% annual growth in workloads for the public cloud versus an 8.9% growth for "on- premise" computing workloads is expected. It is predicted that the global market for cloud equipment will reach $79.1 billion by 2018.Just enough operating systems (JeOS) will further increase the dependency on cloud. Hence we can conclude that cloud has a bright future.

We have generated an encryption architecture based on three encryption algorithms RSA, tokenization and digital signature and implemented the algorithm.

Its main advantage is that it uses Public Key encryption. This means that our text will be encrypted with someone's Public Key (which everyone knows about). However, only the person, it is intended for; can read it, by using their private key (which only they know about). The encrypted data passes through the tokenization phase. The process finds the tokens of previously encrypted data. Then, algorithm finds the digital signature of each token. So that each token of the encrypted data gets signed. Instead of one string (which can have only one private and its corresponding public key), all the tokens have their unique private and public key. Hence, here a complication of keys occurs which is not easy for an attacker to break it

References

Neha Tirthani Ganesan R, Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography,

Vahid Ashktorab (2012), Seyed Reza Taghizadeh (2012), Security Threats and Countermeasures in Cloud Computing, *International journal of application or innovation in engineering and management*, Vol 1, Issue 2, October 201

Chimere Barron (2013), Huiming Yu (2013) and Justin Zhan (2013), Cloud Computing Security Case Studies and Research, *Proceedings of the world congresson engineering* 2013 Vol.

Amani S. Ibrahim (2010), James Hamlyn- Harris (2010) and Joah Grundy (2010) Emerging Security Challenges of Cloud Virtual Infrastructure *APEC 2010 Cloud Workshop, Sydney*, Nov. 2010

Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing.

Dimitrios Zissis (2012), Dimitrios Lekkas (2012), Addressing cloud computing security issues, *Future generation computer systems 28(2012)583-592 , www.elsevier.com/locate/fgcs*

Chittaranjan Hota (2011), Sunil Sanka (2011), Srijith K. Nair(2011) Capability-based Cryptographic Data Access Control in Cloud Computing, *International journal of advanced networking and applications*, Vol. 03; Issue 03 (2011)

Kangchan Lee (2012), Security Threats in Cloud Computing *Environments ,International journal of security and its applications* Vol. 6, No.4, October 201

Sara Qaisar (2012), Kausar Fiaz Khawaja (Corresponding Author) (2012), Cloud computing: network/security threats and countermeasures, *Interdisciplinary journal of contemporary researcin Business*, Vol. 3, No. 9, January 2012

Mohammed A. AlZain (2012), Eric Pardede (2012), Ben Soh (2012), James A. Thom (2012), Cloud Computing Security: From Single to Multi-Cloud, *45th Hawaii international conference on system on system Sciences DOI* 10.1109/HICSS.2012.153 (2012)

P.Senthil (2012), N.Boopal(2012), R.Vanathi (2012), Improving the Security of Cloud Computing using Trusted Computing Technology, *International journal of modern engineering research*, Vol. 2 Issue 1, Jan-feb 2012 pp-320-325

Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito, Security and Cloud Computing: InterCloud Identity Management Infrastructure

Anup Mathew (2012), Survey Paper on Security & Privacy Issues in Cloud Storage Systems The Institute for Computing, *EECE 571B, Term Survey Paper*.

Amar Gondaliya (2011), Hasmukh Goswami(2011), Security in Cloud Computing, Ahmedabad,Technical UNISYS *technical Paper Contest* 2011

Keiko Hashizume1(2013), David G Rosado(2013), Eduardo Fernández-Medina(2013) and Eduardo B Fernandez(2013), Hashizume(2013), An analysis of security issues for cloud computing, *et al. Journal of Internet Services and Applications*, 4:5,2013

Santosh Kumar(2012) and R. H. Goudar(2012), Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications*: A Survey*, *International Journal of Future Computer and Communication*, Vol. 1, No. 4.

John C. Roberts II, Wasim Al-Hamdani, Who Can You Trust in the Cloud? A Review of Security Issues Within Cloud Computing,

Nariman Mirzaei(2008), Cloud Computing, Fall

Pankaj Arora, Rubal(2012), Chaudhry Wadhawan(2012)

Satinder Pal Ahuja(2012), Cloud Computing Security Issues in Infrastructure as a Service, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 1, January 2012 ISSN: 2277 128X

Uli Kunesch Fasanenweg, White Paper cloud Computing, Alternative sourcing strategy for business, *T-Systems Enterprise services GmbH*

Anthony Bisong (2011) and Syed (Shawon) M. Rahman(2011) An overview of the security concerns in enterprise cloud computing, *International Journal of Network Security & Its Applications (IJNSA*), Vol.3, No.1

An Osterman Research (2012), A Cloud-Client Architecture Provides Increased Security at Lower Cost *White Paper Published*

Anand Nayyar(2011), Private Virtual Infrastructure (PVI) Model for Cloud Computing, *International Journal of Software Engineering Research & Practices* Vol.1, Issue 1

Digital Signatures CCA Controller of Certifying Authorities Ministry of Communications & Information Technology

The RSA Algorithm, JooSeok Song 2007. 11. 13.

http://docs.oracle.com/javase/tutorial/security

http://www.infoworld.com/t/encryption/ibm homomorphic-encryption-could-revolutionize-security-233323

http://news.ncsu.edu/releases/wmsjianghypersafe

http://blog.pluralsight.com/what-is-hypervisor