IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

MULTI TENANCY SECURITY IN CLOUD COMPUTING

Manjinder Singh*, Charanjit Singh
* M-Tech Student, RIMT-IET MandiGobindgarhA.P CSE Dept, RIMT-IET MandiGobdindgarh R I M T-I.E.T G.T Road MandiGobindgarh

DOI: 10.5281/zenodo.438116

ABSTRACT

The word Cloud is used as a metaphor for the internet, based on standardised use of a cloud like shape to denote a network. Cloud Computing is advanced technology for resource sharing through network with less cost as compare to other technologies. Cloud infrastructure supports various models IAAS, SAAS, PAAS. The term virtualization in cloud computing is very useful today. With the help of virtualization, more than one operating system is supported with all resources on single H/W. We can also say that we acquired single server but we used it for multiple functions(Web Server, database server, Application Server, DNS Server, DHCP Server). One more asset of cloud computing is Multi Tenancy. Sharing of one database to many tenants or we can say users is known as multi tenancy. Cloud computing customize the requirements of user and u r able to pay as per use. Network applications share through multi tenancy for various users but security of data is basic issue. This paper discusses about the security with more encryption routines and upgrades performance with network route optimization.Due to increase in performance and security, more number of people attract towards CLOUD COMPUTING. Virtualization is a term of cloud computing. Virtualization is a very new technology in computer technologies. With the help of virtualization share the resources software and hardware. Best example of virtualization is THIN CLIENT technology, which runs more than one client with one server. Desktop virtualization shares the desktop with other thin client. Security and Performance issues link with desktop virtualization also. HP + Microsoft launch one server (H/W provided by HP and S/W provided by Microsoft Multipoint Server edition).

KEYWORDS: Cloud Computing, Virtualization, SAAS, Multi tenancy, Security, RSA.

INTRODUCTION

Today technology changes at very fast speed and our requirements are also changed due to storage and processing speed of various applications which we use on computer technology. Cloud computing is one main solutions of this problem. Architecture of client server is supported by cloud computing and with the support of distinct models, we can share resources according to our requirements. Suppose if we are using only one service of cloud, then we will pay money just for that particular service, not for the whole framework and architecture. Suppose one person decided to launch a website than person purchase H/W & S/W for it but in case of cloud computing person do not use the require any purchasing person develop his website and store on cloud server live example of this situation is AMAZON. AMAZON server storage space is available for any service (Website or database server connectivity to any website). According to their service roles, cloud computing models are used. For example, we share on software through SAAS model. Platform sharing through PAAS and infrastructure through IAAS.

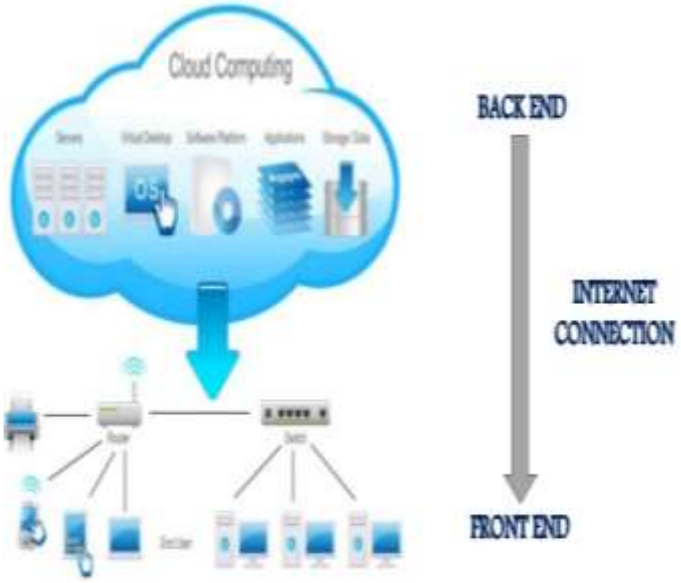

Figure 1. Architecture of cloud computing environment

Cloud Service Deployment and Consumption Models

Public Cloud:

Public clouds are provided by a designated service provider and may offer either a single tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The nominated service provider generally owns and maintainsthe physical infrastructure and this infrastructure is located within the provider's data centres (off premises). Same infrastructure pool is shared by all the customers with limited configuration, securityprotections, and availability variances. One of the assets of public clouds is that they may be biggerthan an enterprise cloud, and thus they provide the capability to scale consistently on demand.

Private Cloud:

An organization provides private clouds or their designated services and offers a single-tenant (dedicated) operating environment with all the betterment and functionalities of flexibility andaccountability/utility model of cloud. The private clouds desire to address concerns on data security and offer more control, which is commonly lacking in a public cloud. Two alternatives of private clouds are there:

(i) on-premise private clouds and
(ii) Externally hosted private clouds

The on-premise private clouds, alsoknown as internal clouds are hosted within one's own data canter. A morestandardized process and protection is provided by this model, but it is limited in aspects of size and scalability. There wouldalso the need to acquire the capital and operational costs for the physical resources in IT departments. It is appropriated for the applications that desires security, complete control and configurability of the infrastructure. As the name signifies, the externally hosted private clouds are hosted externally with a cloud provider.

Hybrid Cloud:

Hybrid clouds are a composition of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across diversecloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. Service providers can utilize third party cloud providers with a hybrid cloud, in a full or sectional manner, thereby raising the computing flexibility. The hybrid cloud model is ableof providing on-demand, externally provisioned scale. The capability to amplify a private cloud with the resources of a public cloud can be used to administer any unpredicted surges in workload.

Cloud Computing Implementation Software Applications With Saas

Computer network play a big role in the implementation of any software on cloud computing. Network has possibly highest impact on cloud deployment's success because users needed to access remote locations. Because of this reason,a positive approach is desired by cloud computing towards network. Network speed depends on its design and attaches devices (LAN cards, Switches (Manageable and Non Manageable), Router. Cloud computing involves SOA (Service Oriented Architecture) and virtualization of Hardware and Software.

SAAS model of cloud computing implements install and operate application software in the cloud and the software is accessed by cloud users from cloud clients. Cloud computing delivers a single application through the browser to thousands of customers using multi tenancy architecture. SAAS is an application which is hosted on a remote server and accessed over internet. SAAS is model in which application is hosted as a service to customers who access it via the internet software as a service, actually it is software delivery model in which software and associated data are centrally hosted on the cloud.

Virtual Machine (VM):

A virtual machine (VM) is a software implementation of a computing environment in which an operating system or a program can be installed and run on host machine. It typically emulatesaphysical computing environment, but requests for CPU time slot, memory, hard disk, network and other resources are managed by a virtualization layer which translates these requests to the underlying physicalhardware. Virtualization supervises network card for guest operating system that is installed through virtual machine. Network card install by Microsoft Adapter which is same working as original network card we also managed router, NAT through virtualization. Virtualization is a complete solution for today technology, as the technology changes at rapid speed. We can liberate a very big cost of H/W with the help of virtualization. Within a virtualization platform, VMs are created that run on top of a client or server operatingsystem. This operating system is known as the host operating system. For creating many individual, isolated VM environments, virtualization layer can be used or it can also be used to divide the resources of H/W. In case H/W we install more than one O/S on one machine (Server or Workstation). Virtualization softwares or applications are MICROSOFT VIRTUAL PC, VIRTUAL BOX etc. These softwares support all type of applications which run on one general machine. Suppose we have a PC which have 2GB Ram, 500 GB HDD & i3 Processor than easily we run two O/S on this machine, Base O/S Windows & Virtual O/S Linux. Network connectivity b/w these two O/S be same as b/w two PC's. This is best example of resource sharing through virtualization.

Cloud Service Delivery Models

Three archetypal models and the derivative combinations thereof generally describe cloud servicedelivery. The three individual models are often referred to as the "SPI MODEL", where "SPI" referstoSoftware, Platform and Infrastructure (as a service) respectively.

Software as a Service (SaaS):

The capability provided to the consumer is to use the provider'sapplications running on a cloud infrastructure and accessible from various client devices through a thinclient interface such as web browser. In other words, a complete application is offered tothe customer as a service on demand in this model. A single instance of the service runs on the cloud and multiple endusers are services. On the customers' side, there is no need for upfront investment in servers or softwarelicenses, while for the provider, the costs are lowered, since only a single application needs to be hosted and maintained. In summary, in this model, the customers do not manage or control the underlying cloudinfrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Companies such as Google, Sales force, Microsoft,Zohoetc offers SaaS currently.

Platform as a Service (PaaS):

A layer of software or development environment is encapsulated and offered as a service in this model, upon which other more advanced levels of services are built. The customer has the freedom of building his own applications that run on the infrastructure of provider. Hence, acapability is provided to the customer to deploy onto the cloud infrastructure customer-createdapplications using programming languages and tools supported by the provider (e.g., Java, .Net etc.). Although the customer does not manage or control the underlying cloud infrastructure, network servers, operating systems, or storage, but customer has the control over the deployed applications andpossibly over the application hosting environment configurations(Customer also manage Application Access Credentials). To meet manageability and scalabilityrequirements of the applications, PaaS

providers offer a predefined combination of operating systems and application servers, such as XAMP (Windows, Apache, MySql and PHP) platform, restricted J2EE, Ruby etc.
Some examples of PaaS are: Google's App Engine, Force.com etc.

Infrastructure as a Service (IaaS):
This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. Customer is provided with the facilities of rent processing, storage, networks, and other fundamental computing resources, where the customeris capable to deploy and run arbitrary software, which can incorporate operating systems and applications.The customer does not manage cloud serveror we can say cloud infrastructure but has thecontroloveroperating systems, storage, deployed applications, and possibly select networkingcomponents (e.g. firewalls,load balancers etc.). Some examples of IaaS are: Amazon, GoGrid, 3 Tera etc.

Cloud Computing Security And Privacy Issues
This section addresses the core theme of this paper, i.e., the security and privacy-related challenges incloud computing. There are various security concerns for cloud computing as it encircles manytechnologies including networks, databases, operating systems, virtualization, resource scheduling,transaction management, load balancing, concurrency control and memory management. Hence, security concerns are applicable to cloud computing for many of these systems and technologies. Forexample, the network has to be secure that interconnects the systems in a cloud. Furthermore, virtualization paradigm in cloud computing leads to several security concerns. For example, mapping thevirtual machines to the physical machines has to be carried out securely.

Encryption of data as well as assuring that applicable policies are accomplished for data sharing, are included in data security. In addition resource allocation and memory management algorithms have to be secure. Finally, data miningtechniques may be applicable for malware detection in the clouds – an approach which is usually adoptedin Intrusion Detection Systems (IDSs).

For securing data which is transfer through network, cryptographic encryption techniques are certainly the best options. The hard drive manufacturers are now shipping self-encrypting drives that implement trusted storage standardsofthe trusted computing group (Trusted Computing Group's White Paper, 2010). These self-encryptingdrives build encryption hardware into the drive, providing automated encryption with minimal cost orperformance impact. Although software encryption can also be used for securing data, it makes thesystem slower and less secure as it may be possible for an attacker to steal the encryption key fromthe machine without being detected.

Encryption is the best option for securing data in transit as well, because cipher text which is more secure than simple text. Best example of encryption is HTTPS protocol more secures than http. TELNET protocol not supported any encryption technique so plain text transfer through network which is very harmful because any hacker see the plain text data but encrypted data or cipher text more secure. In addition, authentication and integrity protection mechanisms assure that data goes to thatplace only where the customer wants it to go and it is notcustomized while transmission.For any cloud deployment, strong authentication is an essential requirement. User authentication is theprimary basis for access control. Authentication and access control are more necessary than ever in the cloud environment, since the cloud and all of its data are accessible to anyone over the Internet.

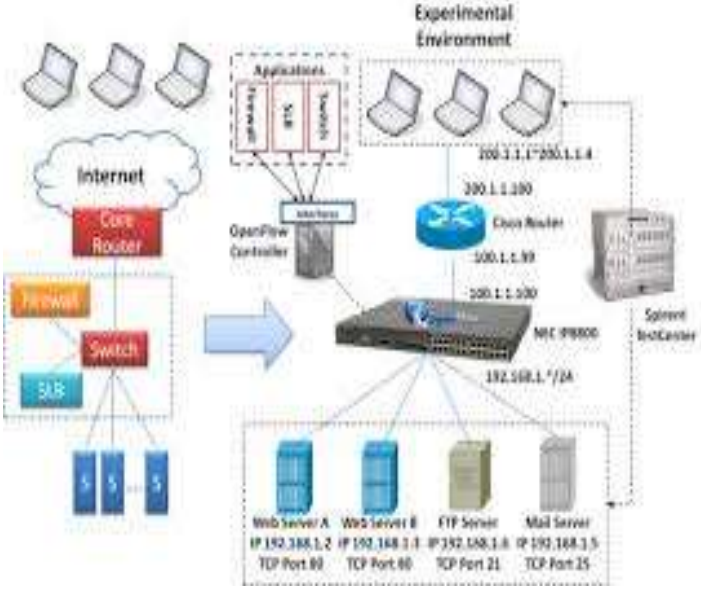

Figure 2. user authentication in cloud computing environment

Security In Cloud Computing Using RSA

.

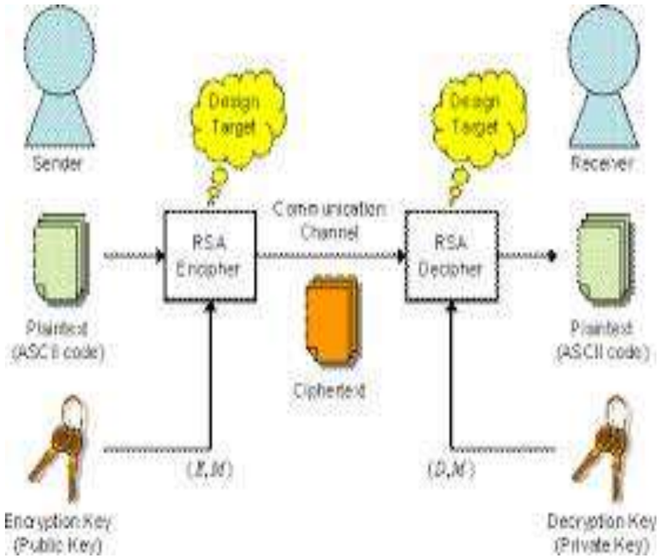

Figure 3. Framework of RSA in Cloud Computing

Let us define some integer parameters: P as a plain text, C as an encrypted text, E as the encryption key, D as the decryption key, and M as modulo number. The encryption can be made by following equation

$$C = PE \quad mod\ M \qquad (1)$$

Where mod expresses a modular operation. On the other hand, the following equation is used for decryption

$$P = CD\ mod\ M \qquad (2)$$

As we can see in Eq. (1) and (2), the RSA encryption system's expression itself is not complicated. At the first step how to define E, D and M. We choose quite large number of two prime factors p and q (p ≠ q) randomly. Then modulo M is defined as M = p × q. From p and q, we define

$$L = LCM\ (p-1, q-1) \qquad (3)$$

Where LCM stands for the least common multiple. The encryption key is chosen as a certain number which is less than and mutually prime with L. Therefore E can be expressed as

$$GCD\ (L, E) = 1 \qquad (4)$$

Where GCD stands for the greatest common devisor. In order to shorten the processing time (computational complexity), E is often chosen to be comparatively small number. Lastly, the decryption key D should gratify the following equation for arbitrary integer number H.

E.D = H. L + 1 ***(5)***

By using above defined E, D and M, encryption and decryption can be carried out according to the Eq.(1) and (2). As you might already recognize it, if the modulo M can be prime factorized, the decryption key D can be surely attained; however, as far as M is chosen as certain hundred digits, prime factorization would take more than 10 years or more even by using a state-of-the-art super computers. It assures the robustness in terms of the RSA algorithm against attacking.

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.

RSA Example

1. Key generation in RSA:

Suppose we choose P=11 and Q=23, find the encryption key E, the decryption key D, and modulo M.

M = P x Q = 253

L = LCM (11-1, 23-1) = 110

According to Eq. (4), E satisfies

GCD (L, E) = 1

Therefore, E=101 is one of the candidate.

If we choose H=56 as an arbitrary integer number, then D=61 according to Eq. (5)

2. Encryption and decryption:

Suppose, to convert Alphabet characters into several integer numbers, we make use of the ASCII code. Encrypt the following plain text into cipher text. Then decrypt this cipher text into the original plain text. Here we encrypt a plain text one character by one character. Normally, a block wise processing is used for it, which means several characters are encrypted as block manner.

Plain text: Enjoy HDL! According to ASCII code, we get

Coded plain text: 69 110 106 111 121 32 72 68 76 33

Applying Eq. (1) into first character 'E', which is 69 in ASCII code, we get

C = PE mod M

C = 69101 mod 253 = 69

This number 69 is the encrypted code in terms of the first character 'E'. The issue in this equation is that huge complexity is desired for power calculation. The solution to this problem could be one of the objectives for better RTL design. The whole plain text can be encrypted in the manner as it was for the first character.

Encrypted (Cipher) text: 69 209 172 122 220 219 193 68 43 176

This cipher text can be decrypted by using Eq. (2). For the first encrypted data '69', we get

P = CD mod M

P = 6961 mod 253 = 69

This is nothing but character 'E' as was in the original plain text. In this way we decrypt other cipher text all together.

Internet Engineering Task Force (IETF):

IETF (IETF Homepage) has inaugurated the Cloud OPS WG (working group on cloud computing and maintenance), which is considering cloud resource management and monitoring currently, and Cloud-APSBOF which has concentrated on cloud applications.

SECURITY SOLUTIONS FOR CLOUD COMPUTING

1. Authentication and Authorization
2. Identity and Access management
3. Confidentiality, Integrity and Availability
4. Security Monitoring and Incident Restore
5. Security Policy Management

PROPOSED WORK

In Multitenant application, data isolation of tenants is a greatissue. So, for security purpose, separate database is granted to each tenant, but it is time consuming and less cost effective. Single database is the best step to diminish these entire consequences,where each row store tenant data with their tenant's id and thus each row gets separated by its id. In this surrounding area,security concerns dart high that misconfigure application codeor an inaccuracy in an admittance control list may put tenantinformation in the danger of thievery and use wrongly. Fordesigning access to the data in database, there are reasonably a smallnumber of tools and technologies available. The newapplications implemented is use for validation and approve of the access request so that only firm rows or fields arechangeable based on security policies that guarantee access isdefensible. In this way,it results in the devaluation of cost and time of implementingdatabase. But still, there is some possibility of dataleakage of one tenant by another tenant. To recover from this insecurity we use the concept of cryptography. Cryptographyis the technique through which encryption/decryption of datagets performed. The RSA algorithm is one of the bestalgorithms of cryptography.

CONCLUSION

In this paper, we give the analysis of data storage incloudcomputing and the security in cloud system. Here, the main concept is to provide integrity to the cloud storage area with distinct data models and security algorithms. Firstly, we present the cloud data storage architecture along withthe cloud data models. Then we suggest the algorithm forcloud security using RSA algorithm. In this method, someimportant security services including key generation encryption and decryption are provided in Cloud Computingsystem. The main objective is to securely store and manage datathat is not controlled by the owner of the data. The data arestored in cloud environment Cloud security here is solved by providing an RSA algorithm.

REFERENCES

[1] S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for CloudComputing (S. Pearson and G. Yee, eds.), Computer Communications and Networks, pp. 3–42, Springer London, 2013.
[2] V. Josyula, M. Orr, and G. Page, CloudComputing: Automating the Virtualized Data Center, Cisco Systems, Inc., Indianapolis, USA, 2011.
[3] F. Liu et al., "NIST Cloud Computing Reference Architecture", National Institute of Standards and Technology, U.S Department of Commerce, Special Publication 500-292, Sep. 2011.
[4] Mell, P. &Grance, T (2011) The NIST Definition of Cloud Computing, (Special Publication 800-145). Gaithersburg MD: National Institute of Standards and Technology.
[5] Singleton D., "It's time for a cloud UIstandard",http://blog.softwareadvice.com/articles/enterprise/its-time-for-a-cloud-ui-standard-1021412/, last retrieved 18 Nov 2013.
[6] Cloud Computing Security Issues in IAAS, Volume 2, Issue 1, January 2012, ISSN: 2277 128X.
[7] Cloud Computing Data Storage and Security Enhancement, Volume 1, Issue 6, August 2012.
[8] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in, cloud Computing", 2010.
[9] Sunita Rani and AmbrishGangal, "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints", (IJCSIT), Vol. 3 (3), 2012, 4302 – 4304.
[10] AlokTripath and Abhinav Mishra," Cloud Computing Security Considerations", IT Division, DOEACC Society, Gorakhpur Centre Gorakhpur, India, 2010, IEEE
[11] "Advance Computer Technology" a book by Dr.Deven shah. Edition-2011.
[12] "Cryptography and Network Security" a book by William Stallings, Fifth Edition
[13] http://www.lsi-contest.com/2008/spec2_e.html.
[14] http://searchcloudsecurity.techtarget.com/tip/Clou d-computing-security-Choosing-a-VPN-type-toconnect-to-the-cloud.
[15] P. Kalpana, "Data Security in Cloud Computing using RSA Algorithm," International Journal of Research in Computer and Communication technology, vol. 1, 2012.