International Journal for Computer Application and Research
Vol. 1 Issue 1, March 2013 (ISSN: 2320-5067)

Security Issues in Cloud Computing

Deepak jain
Student(MCA)
Gitarattan International Business School

Abstract:

Cloud Computing holds the potential to eliminate the requirements for setting up of highcost computing infrastructure for the IT-based solutions and services that the industry uses. It promises to provide a flexible IT architecture, accessible through internet for lightweight portable devices. This would allow many-fold increase in the capacity or capabilities of the existing and new software. In a cloud computing environment, the entire data reside over a set of networked resources, enabling the data to be accessed through virtual machines. Since these data centres may lie in any corner of the world beyond the reach and control of users, there are multifarious security and privacy challenges that need to be understood and taken care of. Also, one can never deny the possibility of a server breakdown that has been witnessed, rather quite often in the recent times. There are various issues that need to be dealt with respect to security and privacy in a cloud computing scenario. This extensive survey paper aims to elaborate and analyze the numerous unresolved issues threatening the Cloud computing adoption and diffusion affecting the various stake-holders linked to it.

Keywords – Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Interoperability, Denial of Service (DoS), Distributed Denial of Service (DDoS), Mobile Cloud Computing (MCC).

1. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it.

The advantages of using cloud computing are:

i) Reduced hardware and maintenance cost,
ii) Accessibility around the globe,
iii) Flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter

Cloud Computing has been defined as the new state of the art technique that is capable of providing a flexible IT infrastructure, such that users need not own the infrastructure supporting these services. This integrates features supporting high scalability and multi-tenancy. This approach is device and user-location independent.

Fig.1 A simple cloud computing model with the three basic cloud services involved

Software as a Service (SaaS) ensures that the complete applications are hosted on the internet and users use them. The payment is being made on a pay-per-use model. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance. In SaaS, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the "Read Lock" or "Write Lock" [1]. Two types of servers are used by SaaS: the Main Consistence Server (MCS) and Domain Consistence Server (DCS). Cache coherence is achieved by the cooperation between MCS and DCS. In SaaS, if the MCS is damaged, or compromised, the control over the cloud environment is lost. Hence securing the MCS is of great importance.

Platform as a service approach (PaaS), the offering also includes a software execution environment. As for example, there could be a PaaS application server that enables the lone developers to deploy web-based applications without buying actual servers and setting them up. PaaS model aims to protect data, which is especially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus the need for security against outage is important to ensure load balanced service. The data needs to be encrypted when hosted on a platform for security reasons [3].

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services, typically using Virtualization technology. With IaaS approach, potentially multiple users use available resources. The resources can easily be scaled up depending on the demand from user and they are typically charged for on a pay-per-use basis. The resources are all virtual machines, which has to be managed. Thus a governance framework is required to control the creation and usage of virtual machines. This also helps to avoid uncontrolled access to user's sensitive information.

cloud services can be deployed in four ways depending upon the customers' requirements:

i) ***Public Cloud****:* A cloud infrastructure is provided to many customers and is managed by a third party [7]. Multiple enterprises can work on the infrastructure provided, at the same time. Users can dynamically provision resources through the internet from an off-site service provider. Wastage of resources is checked as the user pays for whatever they use.

ii) ***Private Cloud****:* Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider [7]. This uses the concept of virtualization of machines, and is a proprietary network

iii) ***Community cloud****:* Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider.

iv) ***Hybrid Cloud****:* A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other.

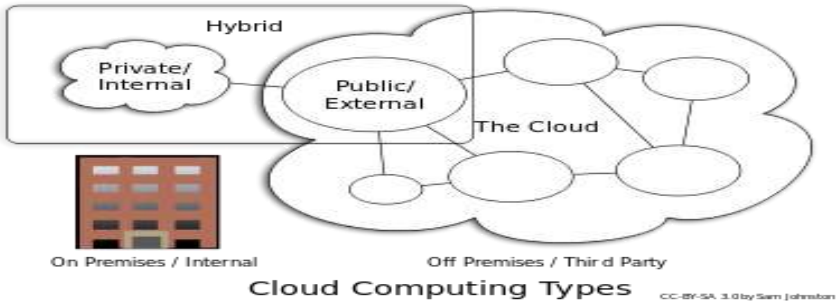

Fig.2 Types of Cloud Computing

Moreover, with the technological advancements, we can see derivative cloud deployment models emerging out of the various demands and the requirements of users. A similar example being a virtual-private cloud wherein a public cloud is used in a private manner, connected to the internal resources of the customer's data-centre . With the emergence of high-end network access technologies like 2G, 3G, Wi-Fi, Wi-Max etc and feature phones, a new derivative of cloud computing has emerged. This is popularly referred as "Mobile Cloud Computing (MCC)". It can be defined as a composition of mobile technology and cloud computing infrastructure where data and the related processing will happen in the cloud only with an exception that they can be accessed through a mobile device and hence termed as mobile cloud computing .

A few state of the art techniques that contribute to the cloud computing are:

i) ***Virtualization:*** It has been the underlying concept towards such a huge rise of cloud computing in the modern era. The term refers to providing an environment able to render all the services, being supported by a hardware that can be observed on a personal computer, to the end users. The three existing forms of virtualization categorized as: Server virtualization, Storage virtualization and Network virtualization have inexorably lead to the evolution of Cloud computing. As for example, a number of underutilized physical servers may be consolidated within a smaller number of better utilized severs.

ii) ***Web Service and SOA:*** Web services provided services over the web using technologies like XML, Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP), and Universal Description, Discovery, and Integration (UDDI). The service organisation inside a cloud is managed in the form of Service Oriented Architecture (SOA) and hence we can define SOA as something that makes use of multiple services to perform a specific task.

iii) ***Application Programming Interface (API):*** Without API's it's hard to believe the existence of cloud computing. The whole bunches of

cloud services depend on API's and allow deployment and configuration through them. Based on the API category used viz. Control, Data and Application API's different functions are being controlled and services rendered to the users.

iv) ***Web 2.0 and mash-up:*** Web 2.0 has been defined as a technology, enabling us to create web pages that don't limit a user to viewing only; in fact it allows the users to make dynamic updates as well. It enables the usage of World Wide Web technology towards a more creative and a collaborative platform. Mash-up is a web application that combines data from more than one source into a single integrated storage tool.

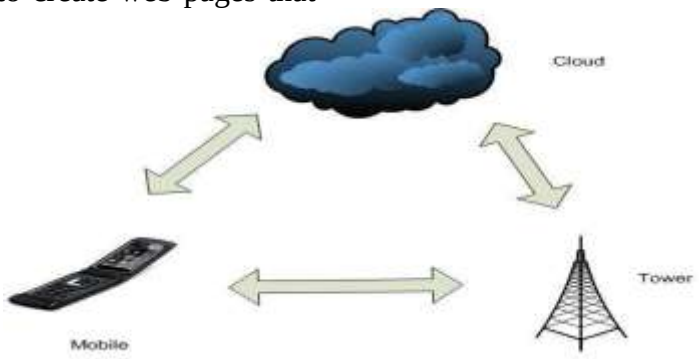

Fig3. A Mobile Cloud Computing Scenario

These were the few technological advances that led to the emergence of Cloud Computing and enabled a lot of service providers to provide the customers a hassle free world of virtualization fulfilling all their demands. The prominent ones are: Amazon-EC2 (Elastic Compute Cloud), S3 (Simple Storage Service), SQS (Simple Queue Service), CF (Cloud Front), SimpleDB, Google, Microsoft, ProofPoint, RightScale, Salesforce.com,Workday, SunMicrosystems etc and each of them are categorised either as one of the three main classifications based on the cloud structure they provide: private, public and hybrid cloud. Each of the above mentioned cloud structure has its own limitations and benefits.

2. THREATS TO SECURITY IN CLOUD COMPUTING

The chief concern in cloud environments is to provide security around multi-tenancy and isolation, giving customers more comfort besides "trust us" idea of clouds [5]. There has been survey works reported that classifies security threats in cloud based on the nature of the service delivery models of a cloud computing system . However, security requires a holistic approach. Service delivery model is one of many aspects that need to be considered for a comprehensive survey on cloud security. Security at different levels such as Network level, Host level and Application level is necessary to keep the cloud up and running continuously. In accordance with these different levels, various types of security breaches may occur. These have been classified in rest of this section.

2.1 Basic Security

Web 2.0, a key technology towards enabling the use of Software as a Service (SaaS) relieves the users from tasks like maintenance and installation of software. It

has been used widely all around. As the user community using Web 2.0 is increasing by leaps and bounds, the security has become more important than ever for such environment .

2.1.1 SQL injection attacks, are the one in which a malicious code is inserted into a standard SQL code and thus the attackers gain unauthorized access to a database and become able to access sensitive information. Sometimes the hacker's input data is misunderstood by the web-site as the user data and allows it to be accessed by the SQL server and this lets the attacker to have know-how of the functioning of the website and make changes into that. Various techniques like: avoiding the usage of dynamically generated SQL in the code, using filtering techniques to sanitize the user input etc to check the SQL injection attacks.

2.1.2 Cross Site Scripting (XSS) attacks, which inject malicious scripts into Web contents have become quite popular since the inception of Web 2.0. Based on the type of services provided, a website can be classified as static or dynamic. Static websites don't suffer from the security threats which the dynamic websites do because of their dynamism in providing multi-fold services to the users.

As a result, these dynamic websites get victimized by XSS attacks.More often either unknowingly or out of curiosity users click on these hazardous links and thus the intruding third party gets control over the user's private information or hack their accounts after having known the information available to them.

2.2 Network Level Security

Networks are classified into many types like: shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. To ensure network security following points such as: confidentiality and integrity in the network, proper access control and maintaining security against the external third party threats should be considered while providing network level security.

2.2.1 DNS ATTACKS

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. 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 evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems.

2.2.2 SNIFFER ATTACKS

These types of attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based

on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network .

2.2.3 ISSUE OF REUSED IP ADDRESSES

Each node of a network is provided an IP address and hence an IP address is basically a finite quantity. A large number of cases related to re-used IP-address issue have been observed lately. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user.

2.2.4 BGP PREFIX HIJACKING

Prefix hijacking is a type of network attack in which a wrong announcement related to the IP addresses associated with an Autonomous system (AS) is made and hence malicious parties get access to the untraceable IP addresses. On the internet, IP space is associated in blocks and remains under the control of AS's. An autonomous system can broadcast information of an IP contained in its regime to all its neighbours.

These ASs communicate using the Border Gateway Protocol (BGP) model. Sometimes, due to some error, a faulty AS may broadcast wrongly about the IPs associated with it. In such case, the actual traffic gets routed to some IP other than the intended one. Hence, data is leaked or reaches to some other destination that it actually should not. An autonomous security system for autonomous systems has been explained in.

2.3 Application Level Security

Application level security refers to the usage of software and hardware resources to provide security to applications such that the attackers are not able to get control over these applications and make desirable changes to their format. Now a days, attacks are launched, being disguised as a trusted user and the system considering them as a trusted user, allow full access to the attacking party and gets victimized. The reason behind this is that the outdated network level security policies allow only the authorized users to access the specific IP address. With the technological advancement, these security policies have become obsolete as there have been instances when the system's security has been breached, having accessed the system in the disguise of a trusted user. With the recent technological advancements, it's quite possible to imitate a trusted user and corrupt entire data without even being noticed.

Hence, it is necessary to install higher level of security checks to minimize these risks. The traditional methods to deal with increased security issues have been to develop a task oriented ASIC device which can handle a specific task providing greater levels of security with high performance. But with application-level threats being dynamic and adaptable to the security checks in place, these closed systems have been observed to be slow in comparison to the open ended systems.

The capabilities of a closed system as well as the adaptability of an open ended system have been incorporated to develop the security platforms based on Check Point Open Performance Architecture using Quad Core Intel Xeon Processors. Even in the

virtual environment, companies like VMware etc are using Intel Virtualization technology for better performance and security base. It has been observed that more often websites are secured at the network level and have strong security measures but there may be security loopholes at the application level which may allow information access to unauthorized users. The threats to application level security include XSS attacks, Cookie Poisoning, Hidden field manipulation, SQL injection attacks, DoS attacks, Backdoor and Debug Options, CAPTCHA Breaking etc resulting from the unauthorized usage of the applications.

2.3.1 SECURITY CONCERNS WITH THE HYPERVISOR

Cloud Computing rests mainly on the concept of virtualization. In a virtualized world, hypervisor is defined as a controller popularly known as virtual machine manager (VMM) that allows multiple operating systems to be run on a system at a time, providing the resources to each operating system such that they do not interfere with each.

As the number of operating systems running on a hardware unit increase, the security issues concerned with those that of new operating systems also need to be considered. Because multiple operating systems would be running on a single hardware platform, it is not possible to keep track of all and hence maintaining all the operating systems secure is difficult. It may happen that a guest system tries to run a malicious code on the host system and bring the system down or take full control of the system and block access to other guest operating systems.

It cannot be denied that there are risks associated with sharing the same physical infrastructure between a set of multiple users, even one being malicious can cause threats to the others using the same infrastructure, and hence security with respect to hypervisor is of great concern as all the guest systems are controlled by it. If a hacker is able to get control over the hypervisor, he can make changes to any of the guest operating systems and get control over all the data passing through the hypervisor.

Various types of attacks can be launched by targeting different components of the hypervisor. Based on the learning of how the various components in the hypervisor architecture behave, an advanced cloud protections system can be developed by monitoring the activities of the guest VMs and intercommunication among the various infrastructure components.

2.3.2 DENIAL OF SERVICE ATTACKS

A DoS attack is an attempt to make the services assigned to the authorized users unable to be used by them. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user. Sometimes, when we try to access a site we see that due to overloading of the server with the requests to access the site, we are unable to access the site and observe an error. This happens when the number of requests that can be handled by a server exceeds its capacity. The occurrence of a DoS attack increases bandwidth consumption besides causing congestion, making certain parts of the clouds inaccessible to the users. Using an Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks. A defence federation is used in for guarding against such attacks. Each cloud is loaded with separate IDS. The different intrusion detection systems work on the basis of information exchange. In case a

specific cloud is under attack, then the co-operative IDS alert the whole system. A decision on trustworthiness of a cloud is taken by voting, and the overall system performance is not hampered.

2.3.3 COOKIE POISONING

It involves changing or modifying the contents of cookie to make unauthorized access to an application or to a webpage. Cookies basically contain the user's identity related credentials and once these cookies are accessible, the content of these cookies can be forged to impersonate an authorized user. This can be avoided either by performing regular cookie cleanup or implementing an encryption scheme for the cookie data .

2.3.4 HIDDEN FIELD MANIPULATION

While accessing a web-page, there are certain fields that are hidden and contain the page related information and basically used by developers. However, these fields are highly prone to a hacker attack as they can be modified easily and posted on the web-page. This may result in severe security violations.

2.3.5 BACKDOOR AND DEBUG OPTIONS

A common habit of the developers is to enable the debug option while publishing a web-site. This enables them to make developmental changes in the code and get them implemented in the web-site. Since these debug options facilitate backend entry to the developers, and sometimes these debug options are left enabled unnoticed, this may provide an easy entry to a hacker into the web-site and let him make changes at the web-site level.

2.3.6 GOOGLE HACKING

Google has emerged as the best option for finding details regarding anything on the net. Google hacking refers to using Google search engine to find sensitive information that a hacker can use to his benefit while hacking a user's account. Generally, hackers try to find out the security loopholes by probing out on Google about the system they wish to hack and then after having gathered the necessary information, they carry out the hacking of the concerned system. In some cases, a hacker is not sure of the target. Instead he tries to Google out the target based on the loophole he wishes to hack a system upon. The hacker then searches all the possible systems with such a loophole and finds out those having the loopholes he wishes to hack upon. A Google hacking event was observed recently when login details of various g-mail users were stolen by a group of hackers in China. These had been some of the security threats that can be launched at the application level and cause a system downtime disabling the application access even to the authorized users.

3.ENSURING SECURITY AGAINST THE VARIOUS TYPES OF ATTACKS

In order to secure the cloud against the various security threats and attacks like: *SQL injection, Cross Site Scripting (XSS) attacks, DoS and DDoS attacks, Google Hacking and Forced Hacking*, different cloud service providers adopt different techniques. A few standard techniques in order to detect the above mentioned attacks are as: Avoiding the usage of dynamically generated SQL in the code, finding the meta-structures used in the code, validating all user entered parameters, disallowing and removal of unwanted data and characters, etc. A generic security framework needs to be worked out for an optimized cost performance ratio. The main criterion to be filled up by the generic security framework are to interface with any type of cloud environment, and to be able to handle and

detect predefined as well as customized security policies.

A similar approach is being used by Symantec Message Labs Web Security cloud that blocks the security threats originating from internet and filters the data before they reach the network. Web security cloud's security architecture rests on two components:

a. *Multi layer security:* In order to ensure that data security and block possible malwares, it consists of multi-layer security and hence a strong security platform.

b. *URL filtering:* It is being observed that the attacks are launched through various web pages and internet sites and hence filtering of the web-pages, ensures that no such harmful or threat carrying web page gets accessible. Also, content from undesirable sites can be blocked.

Table 1: *Comparative Analysis for Strengths and Limitations of Some of the Existing Security Schemes*

Security Scheme	Suggested Approach	Strengths	Limitations
Data Storage Security	Uses homomorphic token with distributed verification of erasure-coded data towards ensuring data storage security and locating the server being attacked.	1. Supports dynamic operations on data blocks such as: update, delete and append without data corruption and loss. 2. Efficient against data modification and server colluding attacks as well as against byzantine failures.	The security in case of dynamic data storage has been considered. However, the issues with finegrained data error location remain to be addressed
User identity safety in cloud computing	Uses active bundles scheme, whereby predicates are compared over encrypted data and multiparty computing	Does not need trusted third party (TTP) for the verification or approval of user identity. Thus the user's identity is not disclosed. The TTP remains free and could be used for other purposes such as decryption.	Active bundle may not be executed at all at the host of the requested service. It would leave the system vulnerable. The identity remains a secret and the user is not granted permission to his reque
Trust model for Interoperability and security in cross cloud	1. Separate domains for providers and users, each with a special trust agent. 2. Different trust strategies for service providers and customers. 3. Time and	1. Helps the customers to avoid malicious suppliers. 2. Helps the providers to avoid cooperating/ serving malicious users.	Security in a very large scale cross cloud environment. This scheme is able to handle only a limited number of security threats in a fairly small environment.

	transaction factors are taken into account for trust assignment.		
Virtualized defence and reputation based trust management	1. Uses a hierarchy of DHT-based overlay networks, with specific tasks to be performed by each layer. 2. Lowest layer deals with reputation aggregation and probing colluders. The highest layer deals with various attacks.	Extensive use of virtualization for securing clouds	The proposed model is in its early developmental stage and needs further simulations to verify the performance
Secure virtualization	1. Idea of an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware is proposed. 2. Behaviour of cloud components can be monitored by logging and periodic checking of executable system files	A virtualized network is prone to different types of security attacks that can be launched by a guest VM, an ACPS system monitors the guest VM without being noticed and hence any suspicious activity can be blocked and system's security system notified.	System performance gets marginally degraded and a small performance penalty is encountered. This acts as a limitation towards the acceptance of an ACPS system.
Safe, virtual network in cloud Environment	Cloud Providers have been suggested to obscure the internal structure of their services and placement policy in the cloud and also to focus on side-channel risks in order to reduce the	Ensures the identification of adversary or the attacking party and helping us find a far off place for an attacking party from its target and hence ensuring a more secure environment for the other VMs.	If the adversary gets to know the location of the other VMs, it may try to attack them. This may harm the other VMs in between.

	chances of information leakage.		

Every cloud service provider has installed various security measures depending on its cloud offering and the architecture. Their security model largely depends upon the customer section being served.

One of the security measures implemented by SalesForce.com to avoid unauthorized access to its platform is sending a security code to the registered customer every-time, the same account is accessed from a different IP-address and the user needs to provide the security code at the time of logging in.

It is equally important to secure the data in transit and security of transmitted data can be achieved through various encryption and decryption schemes. In such a scenario, even if the data gets into the hands of a hacker, he won't be able to make any unauthorized use until he knows how to decrypt it. A few of the encryption-decryption techniques include private and public key encryption. In a symmetric key (private key) encryption such as: DES, Triple DES, RC2, RC4 etc, the same key is used for encryption and decryption. Before the data is transferred, the key is shared between both the receiver and the sender. Sender then sends the data after having encrypted it using the key and the receiver decrypts it using the same key.

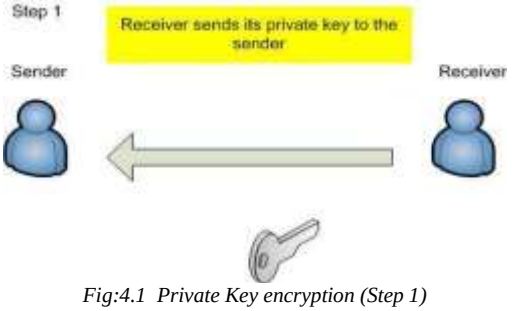

Fig:4.1 Private Key encryption (Step 1)

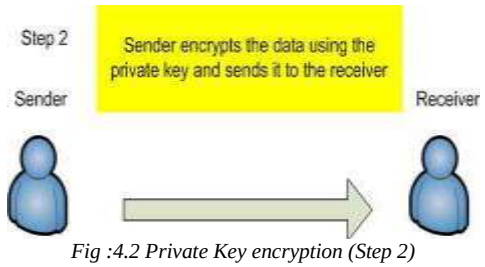

Fig :4.2 Private Key encryption (Step 2)

In case of an asymmetric key algorithm (RSA, DSA, PGP etc), there are two sets of keys known as public key and private key. The keys occur in pairs which means that a specific public key can only be decrypted using the private key linked to it. In such an encryption technique the sender encrypts the data using the public key and then sends it to the receiver which at the receiving end makes use of corresponding private key to decrypt the same.

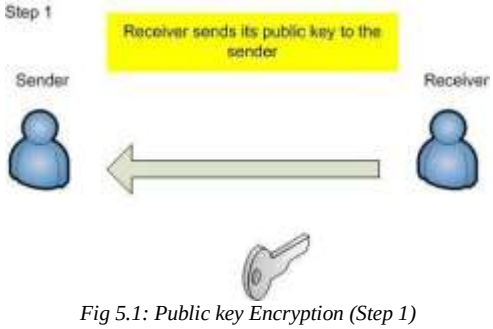

Fig 5.1: Public key Encryption (Step 1)

Hence, we can see that although Public key encryption may take a bit more processing time in comparison to the private key encryption, but in cases where security is more of a concern rather than the speed, public-key encryption provides more secure data transmission in comparison to private-key encryption. Security issues in a virtualized environment wherein a malicious virtual machine tries to take control of the hypervisor and access the data belonging to other VMs have been observed and since traffic passing between VMs doesn't travel

out into the rest of the data-centre network and hence cannot be seen by regular network based security platforms

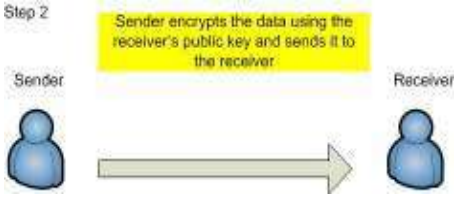

Fig 5.2: Public key Encryption (Step 2)

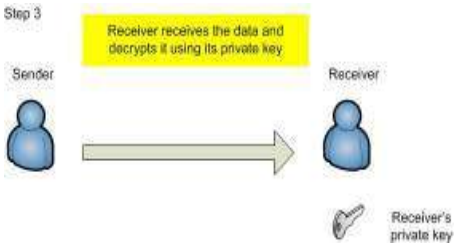

Fig 5.3: Public key Encryption (Step 3)

Hence, there is a need to ensure that security against the virtual threats should also be maintained by adopting the methodologies such as: keeping in check the virtual machines connected to the host system and constantly monitoring their activity, securing the host computers to avoid tampering or file modification when the virtual machines are offline, preventing attacks directed towards taking control of the host system or other virtual machines on the network etc. A security model wherein a dedicated monitoring system taking care of the data coming in and out of a virtual machine/machines functional in a virtualized environment on a hypervisor can be presented as shown below:

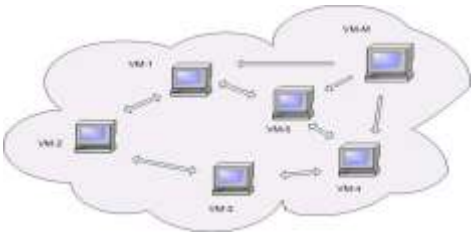

Fig 6: Security Model in a Virtualized Environment

As can be seen from the above shown security model, a Virtual machine monitor can be placed in a virtual environment which will keep track of all the traffic flowing in and out of a virtual machine network. And in case if there is any suspicious activity observed, the corresponding virtual machine may be de-linked or blocked and hence maintaining the security of the virtualized network.

The security breach of Twitter and Vaserv.com (via a zero-day vulnerability) last year and the data breach at Sony Corporation and Go-Grid [6], this year, compromising 100 million customers' [4], data have made it quite clear that stringent security measures are needed to be taken in order to ensure security and proper data control in the cloud.

Thus we see that the security model adopted by a Cloud service provider should safeguard the cloud against all the possible threats and ensure that the data residing in the cloud doesn't get lost due to some unauthorized control over the network by some third party intruder.

4.Conclusion

Cloud Computing is the future for the coming generation architecture of IT enterprise. IT has revolutionized the computing or IT world but there is some threats related to its security from network level to application level security threats. To keep it secure, these threats need to be controlled. Threats like leakage of confidentiality and integrity of data. User must confirm the confidentiality and integrity of data before buying the storage space from the cloud provider. Auditing of cloud at regular intervals need to be done for preventing the external threats. Cloud providers must ensure that human errors on their part should be minimized. In this paper various security concerns for Cloud computing environment from multiple

perspective and the solutions to prevent them have been presented.

5.References

[1]. Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu, "SaaAS - The Mobile Agent based Service for Cloud Computing in Internet Environment," Sixth International Conference on Natural Computation, ICNC 2010, pp. 2935-2939, IEEE, Yantai, Shandong, China, 2010. ISBN: 978-1-4244-5958-2.
[2]. Lori M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy Journal, vol. 7, issue. 4, pp. 61-64, July- Aug 2009, ISSN: 1540-7993.
[3]. John E. Dunn, "Spammers break Hotmail's CAPTCHA yet again", Tech-world, 16th Feb. 2009.
[4]. Czaroma Roman, "Sony Data Breach Highlights Importance of Cloud Security," Cloud Times, May 9, 2011.
[5]. "Security Consideration for Cloud Ready Data-Centres," Juniper Networks, Oct. 2009.
[6]. Go-Grid Security Breach, April, 2011.
[7]. R.L Grossman," The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
[8]. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal ," A Survey on Security Issues in Cloud Computing"