Cloud Computing Security Aspects, Vulnerabilities and Countermeasures

Sarang V. Hatwar
CSE Department
SGGSIE&T, Nanded-431606

R. K. Chavan
CSE Department
SGGSIE&T, Nanded-431606

ABSTRACT
Security issue in cloud computing is an active area of research. Thousands of users are connecting to a cloud daily for their day to day work. Unfortunately they are ignorant about the risk involved while doing transactions on the internet. End user systems as well as cloud based data centers must be able to overcome the threats due to Viruses, Trojan and Malware etc. This paper highlights the major security threats in cloud computing system and introduce the most suitable countermeasures for these threats. Threats are classified according to different perspectives, providing a list of threats. In this article some effective countermeasures are enlisted and discussed.

General Terms
Network security, Cloud security.

Keywords
Cloud computing, security, vulnerabilities/threats and countermeasures.

1. INTRODUCTION
Cloud computing is a domain of using a network where remote servers are hosted to store, manage, and process data at very large scale. It is used for services to provide improved reliability, availability and scalability. The main goal of cloud computing from supplier's point is combination of hardware & software connected to reduce interruption on devices over network without changing user's context. It has a layering mechanism between software, networking and storage, such that every portion can be easily designed, executed, verified and run independently from consequent layers [1]. Figure 1 shows typical infrastructure of cloud computing.

Why enterprises should use cloud computing? [2]

- It has ability to scale up on demand IT capacity
- It has ability for managing large data sets
- It aligns IT resources directly with cost
- It helps in improving IT effectiveness by reducing operational cost
- It places business volatility into single domain

Why enterprises should be careful about cloud? [2]

- Due to nature and level of security threats involved in cloud environment
- It may cause lock-in due to proprietary technology
- It may cause network latency by using internet to use some cloud applications
- In some cases cloud provider may cost more than on-premises systems
- It may be problematic while integrating on-premise system and cloud based system

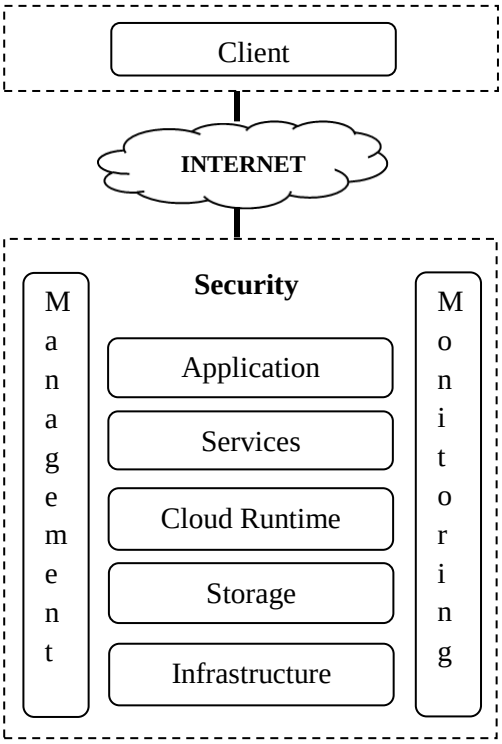

Fig 1: Infrastructure of cloud computing

However cloud computing must provide better utilization of resources by making use of virtualization. Also, it could help to take as much work load from clients even though it is having security related issue. The underlying technology that is used by cloud computing itself provides foremost security risk. This paper describe various security threats along with countermeasures in cloud computing environment. Section 1 gives overview of infrastructure of cloud computing environment. Section 2 deals with security aspects to be focused in cloud computing. Section 3 deals with security threats and challenges in cloud computing. Section 4 deals with security countermeasures. Section 5 delivers a conclusion for the paper.

2. CLOUD COMPUTING SECURITY ASPECTS

2.1 Availability
The objective of availability for cloud framework is to guarantee that thousands of clients can utilize the cloud services irrespective of their location and time. Two methodologies, hardening and redundancy, are mostly used to improve availability of cloud framework and applications facilitated on it. Virtual machines (VM's) are used by numerous cloud computing suppliers to provide cloud

framework and platform. For instance, Amazon Web Service provide EC2, S3 using Xen [3], and Skytap [4] offers virtual lab administration application depending on hypervisors, e.g., Xen [3], VMware [5], Microsoft Hyper-V [6] and KVM [7], etc. That is motivation behind why cloud administration provider can serve resources (e.g., CPU cycles, memory) from Amazon on demand to the cost of use as far as solitary unit. Therefore the main component to host these services is VM. Typically, in cloud environment whenever a user places a request for some service a new virtual machine is created to cater to the requests of the user. If this VM crashes a new VM can be created immediately without apparent disruption in the services. Such VM can be used easily to provide on demand services for very large number of clients. An overview of the virtual machine as shown in Figure 2.

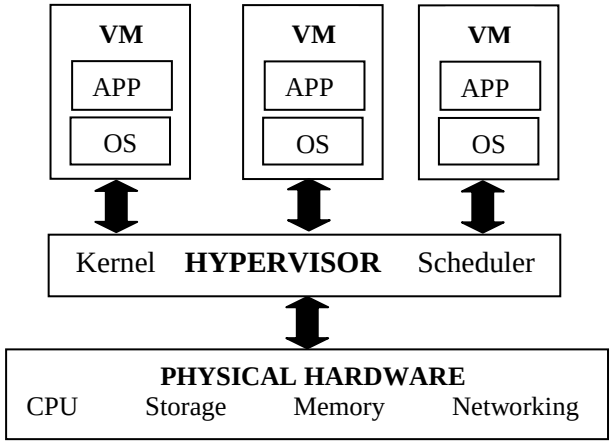

Fig 2: Virtual machine as infrastructure

2.2 Confidentiality

A method of keeping client's data secret is known as confidentiality. Cloud computing system offerings like its infrastructures and applications are generally based on public network. The fundamental requirement of cloud system is to keep user's confidential data very secure. There are two fundamental methodologies,

- Physical isolation
- Cryptography

Encrypting data before setting it in a cloud may be much more secure than unencrypted data in a nearby local data centre. This methodology was effectively utilized in [8].

2.3 Privacy

Another important issue for cloud environment is privacy. In terms of user trust and legal agreement, privacy need to be considered at every designing phase. While designing cloud services by software engineers, the key challenge they face is to decrease privacy risk as well as to ensure legal agreement. Guidelines are suggested for designers, architectures and testers of cloud system [9] as minimize personal information stored and sent over cloud system, maximize client control, allow client verdict, protect individual data in the cloud, specify and limit the motivation behind utilization of information and provide criticism.

2.4 Data Integrity

Data integrity in cloud system means to preserve integrity of information i.e., not lost or altered by unauthorized clients. Moreover, cloud computing system usually gives massive data processing capability.

Figure 3 shows typical delivery model of cloud computing. In such networks, a commonly used technique for data integrity is digital signature. These distributed file systems (e.g., GFS [10], HDFS [11]) usually partition the data in large volumes into set of blocks, each of them having a default size (e.g., 64MB, 128MB). When a block of the data is physically stored, a digital signature is attached to it. For future integrity testing this signature will be helpful. Digital signature help to recover data from corruption.

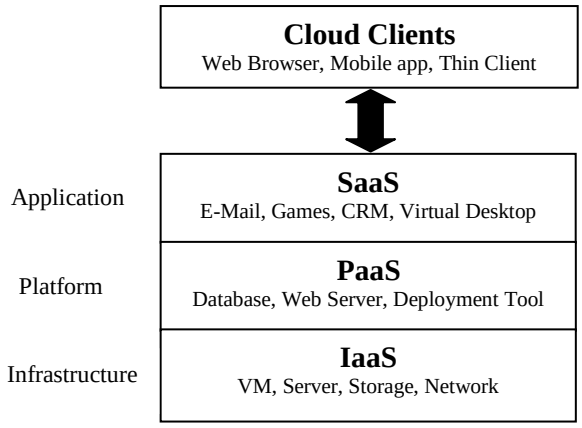

Fig 3: Delivery model of cloud computing

2.5 Identity and Access Management (IAM)

The service providers like Gmail, Yahoo Mail etc., require the username and password to use their services, but they are vulnerable to phishing attacks. IAM can be used to deal with this problem. It is a framework for business processes for managing electronic identities. It supports management of multiple digital identities with their roles, authentication, authorization and privileges. Identity management system has different components like Identity authentication, Directory services, Password administration, Access management, User provisioning, Federated identities and Roles management [12].

2.6 Monitoring and Control of Cloud

Control in cloud system intend to control utilization of system, including cloud applications, infrastructure and information. Cloud computing system dependably includes distributed computation on different large scale information sets. Every web client has ability to contribute his or her individual work to cloud systems which are present on the opposite side of the web. For instance, a client click stream over a set of webs e.g., Amazon book store, Google search web pages, etc., can be utilized to give attentive advertisement. Future healthcare applications may utilize an individual's DNA sequence which is caught by clinics to create custom-made drugs and other customized medicines. At the point when all these individual information are stored in cloud computing system environment, clients of cloud computing system may confront numerous hazards to their personal information. Consequently, effective and powerful control over information access in cloud computing system as well as practice of controlling applications or services facilitated on cloud will improve the security of cloud systems. Monitoring should not be intrusive and must be limited to need of cloud provider in order to run their facility.

2.7 Compliance

Cloud service providers (CSPs) and their clients to address emerging requirement and advancement of cloud business models make use of a programmatic approach to monitor and compliance. CSP's need to implement a powerful inside control monitoring function associated with strong outside assessment process to increase efficiency and risk management. To gain comfort over their in-cloud exercises, CSP clients need to define their control prerequisites, comprehend their CSP's internal control monitoring courses of action, make analysis of outside audit reports and appropriately accomplish responsibility as clients [13].

3. CLOUD COMPUTING SECURITY THREATS

Cloud computing environment is not different from an individual client machine. It is exposed to the same kind of threats as individual machines. Moreover security problems are aggravated due to the nature of cloud environment. Thousands of virtual machines (VM) are running simultaneously in the cloud setup. The threats encountered by the individual machines are more or less responsible for the overall security problems of the cloud environment.

3.1 Threats Identified by "Cloud Security Alliance" (CSA) [14]

Cloud security alliance is a community which looks after the security aspects of the cloud environment and publishes types of the threats from time to time.

3.1.1 Invective and Wicked Use of Cloud Computing

It is the top risk recognized by the cloud security alliance (CSA) [14]. A straightforward case of this is utilization of botnets to spread spam and malware as shown in Figure 4. Intruders can invade a public cloud and figure out how to transfer malware to large number of PCs. This utilizes the power of cloud infrastructure to assault different machines.

3.1.2 Malevolent Insiders

The malevolent insider hazard is one that increases significantly as numerous suppliers still don't disclose how they hire individuals, how they give access to resources for them or how they monitor them. For this situation, it is important to secure cloud offering, compliance reporting and breach notification which help to provide transparency.

3.1.3 Shared Technology Susceptibilities

Infrastructure sharing is an existence for IaaS suppliers. Disappointingly, the segments on which this infrastructure is based were not intended for that. To guarantee that client don't intrude on each other's "zone", strong compartmentalization and monitoring is needed.

3.1.4 Unprotected Application Programming Interfaces (APIs)

APIs are used by clients to make use of services offered by cloud environment. APIs should have strong authentication, encryption, activity monitoring methods and access control. These are essential in the case when outsiders make use of cloud applications and services.

3.1.5 Information Loss

Data is always in risk of being stolen or lost by deleting it without backup, by loss of the encryption key or getting access by unauthorized users. This is one of the top concerns toward organizations, in light of the fact that they remain to lose their reputation as well as committed by law to keep data safe.

3.1.6 Service, Account and Traffic Hijacking

Cloud users need to be aware of service, account and traffic hijacking issue. This hazard ranges from man in the middle attacks, spam campaigns, phishing attacks to DOS attacks. Phishing is a type of attack where attacker create replica of existing webpage to fool users by intending them to submit their personal, financial credentials to what they think that it is provider's original website [15].

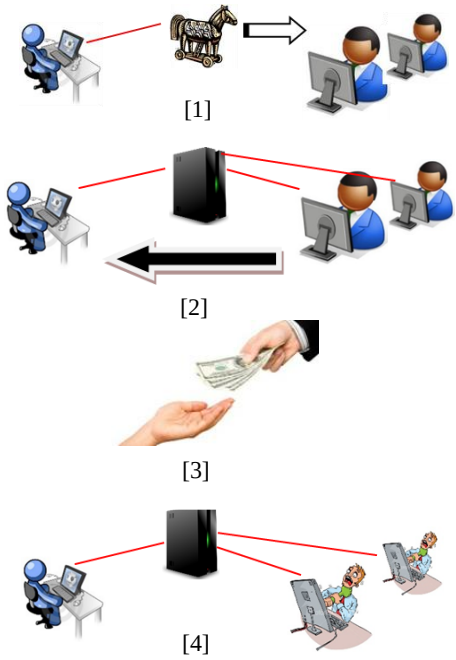

Fig 4: Working of Botnets

3.2 Security Threats Inherited from Networking Perspectives

There are some risky kind of threats which are not particular to cloud environment, but launched immensely in cloud system. This is because of cloud system characteristics and their generality. These hazards are recorded beneath:

3.2.1 Cross Site Scripting (XSS) Attacks

In this kind of assault noxious script is injected into web. There are two strategies of XSS attack: Stored XSS and Reflected XSS.

In Stored XSS, the noxious code is stored permanently in an asset handled by web application [16]. On the other hand, in Reflected XSS, the noxious code is not stored permanently. Indeed it is instantly returned back to the client [16].Working of XSS is as shown in Figure 5.

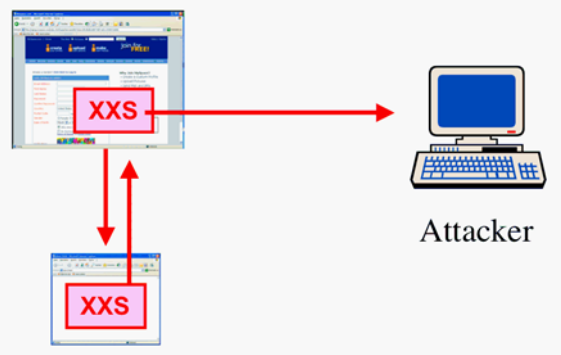

Fig 5: Working of XSS attack

3.2.2 Sniffer Attacks

These kind of assaults are propelled by applications which can catch packets streaming in a network. If the information that is being exchanged through these packets are not encrypted, it can be perused. A sniffer program, through the network interface card (NIC) guarantees that information or traffic attached to different frameworks on the network additionally gets recorded.

3.2.3 SQL Injection Attacks

A harmful code is embedded into a standard SQL query. Therefore attacker gets an illicit access to a database. Attacker is capable to access or change some sensitive information of any cloud user or organization.

3.2.4 Denial of Service (DOS) Attacks

An effort to make network services unavailable to approved users is called as DoS attack. In such an assault, the server delivering services are overwhelmed by countless requests. Thus services cannot be made available to approved clients. Sometimes, when user attempt to access a site he observes that he is unable to access the site and an error massage is displayed. It is due to over-burdening of the server with large number of requests to access the site.

3.2.5 Man-in-the-Middle Attacks

In such an assault, an intruder tries to meddle in a continuous discussion between sender and receiver to infuse false data and to have knowledge of the critical information exchange between them as shown in Figure 6.

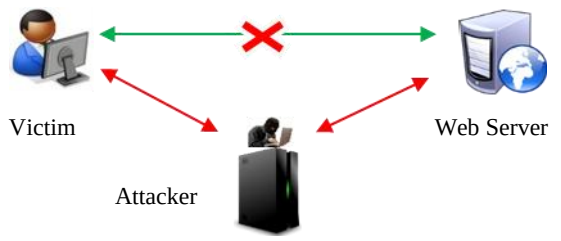

Fig 6: Working of Man in the middle attack

3.2.6 Distributed Denial of Service (DDoS) Attacks

Extended form of DoS attack is DDoS attack as presented in Figure 7. DDoS attack make use of many machines and internet connections. Attacker uses a group of agents to send DDoS attack commands repeatedly to the target system. Sudden traffic can lead to load the website very slowly to their intended users. Sometimes this traffic is so high that it shuts down the site completely.

3.2.7 Reused IP Addresses

At the point when a specific client moves out of a network, then that IP address (prior) is assigned to another new client. However the old IP address is being relocated to another client has the possibilities of getting information by some other client. This fact is not declined as the DNS cache holds the prior IP address. The privacy of the prior client is violated as information belonging to the prior client has open access to some other new client.

3.2.8 Security Issues Related to the Hypervisor

Virtualization is main concept in cloud computing. In virtualization, hypervisor is also known as virtual machine monitor (VMM) which act as controller. VMM is responsible to run multiple operating systems at a time on a host system. As multiple operating systems are running on a single system, it is difficult to supervise all the systems. Hence it is very hard to maintain the security of each one. Sometimes guest OS try to execute a virulent code on host OS. This may lead to take the host system down, take full control host system and obstruct the access to all other guest systems [17].

In kernel virtual machine (KVM) [18] Linux kernel is protected from possible malevolent behavior of VM. Device driver in VM communicate to a user space process (e.g. QEMU) and this process communicate to kernel with the help of regular system call interface. QEMU is exposed to hazards that comes from a malevolent VM. Only low level and limited interfaces can be used to launch attack on it. Hence it make hard to use QEMU as a vector to exploit kernel vulnerabilities in the host machine.

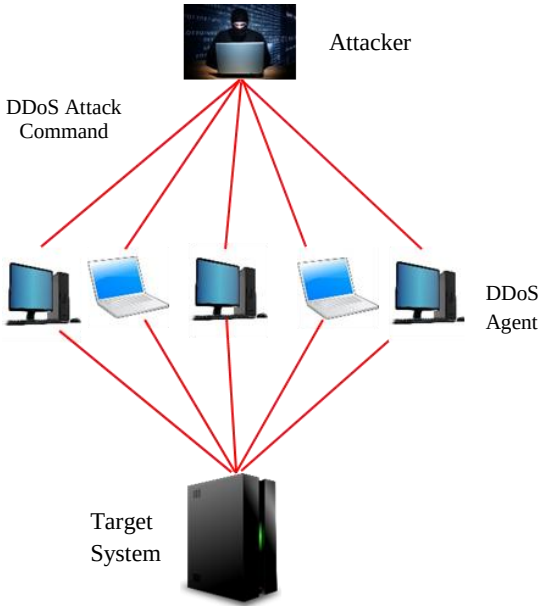

Fig 7: Working of DDoS attack

3.2.9 Google Hacking

Google application engine is the well-known solution supplier in the area of cloud computing. This engine utilizes a distributed architecture known as Google geo-distributed architecture. In this attack, the hacker looks all the conceivable frameworks with an escape clause and discovers those having the provisions he/she wishes to hack upon.

3.2.10 Cookie Poisoning

To have an access of an intruder to a webpage, it involves changing or altering the contents of cookie. User identity

related credentials like username and password etc., are stored in cookies. Once these cookies will be accessible, its content can be changed to approve unauthorized user. Figure 8 illustrates this kind of assault.

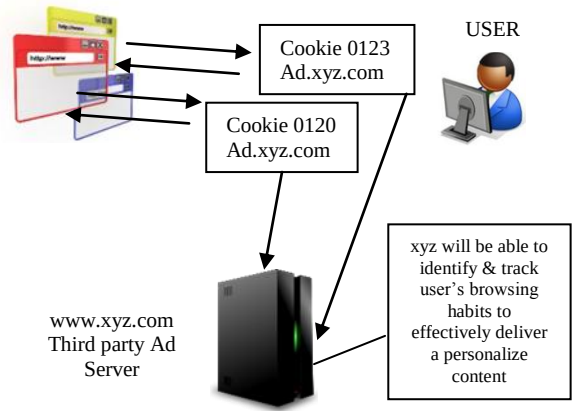

Fig 8: Working of cookie poisoning attack [19]

3.2.11 Cracking CAPTCHA

In recent study, it has been discovered that the spammers are able to break the CAPTCHA, given by the suppliers like Gmail, Hotmail etc., [33]. Spammers utilize audio system which is used to read the CAPTCHA for the visually impaired internet clients [20].

3.3 Additional security threats

3.3.1 Security Concerns in Virtualization Technique

There are two types of virtualization in cloud environment [21]. These are,

- Full Virtualization
- Para Virtualization

In full virtualization, complete hardware architecture is replicated using virtual machines. Again, in para virtualization, an operating system is altered with the goal that it can be run simultaneously with other operating systems. Virtual machine instance isolation guarantees that diverse instances running on the same physical machine are isolated from one another. Nonetheless, offering perfect isolation is not possible by current VMMs. Numerous bugs have been discovered in all prominent VMMs that permit getting into the host OS. All virtualization softwares at least as of now can be abused by harmful clients to sidestep certain security confinements.

3.3.2 Vulnerabilities in OpenStack Cloud

OpenStack is one of the largest open-source cloud computing middleware development community [14]. It has become a preferred cloud framework solution for building private and public clouds within a large number of companies as well as research communities [22].

Vulnerabilities in OpenStack include major issues like Heartbleed, Shellshock, and XEN XSA-108. In Heartbleed [23], an attacker can instruct server to give more data than it is allotted. It attacks a commonly used extension to TLS in the OpenSSL library. This threat can be remotely exploited by the attacker. Shellshock [23] allows an attacker to define environmental variable functions which can be executed to gain unauthorized access to a computer system. Exported bash variables can include function definition. It is remotely exploitable hazard. In XEN XSA-108 [23], attacker can read hypervisor memory, read other guest memory, crash hypervisor and cloud reboot etc., results massive service impact.

3.3.3 Managing Identity

The cloud service provider generate identities to make use of cloud services. Every client utilizes his identity for accessing cloud services. A major issue is unauthorized access to cloud assets and applications. A virulent element can imitate a real client and make use of cloud services. Numerous such malevolent elements acquire the cloud assets prompting un-accessibility of a service for real client. Likewise it may happen that the client crosses his limit at the time of service utilization in the cloud environment. This could be regarding access to safe zone in memory.

Worldwide, 47% of those who are right now utilizing a cloud processing service reported that they have experienced an information security issue with the cloud service used in their organizations during the 12 months [24]. Security lapses are higher in India followed by Brazil as shown in Table 1. Figure 9 shows the status of different countries related to security lapses.

Table 1: Security lapse year wise in different countries

Name	Security Lapse Year Wise	
	2011	2012
India	55%	67%
USA	39%	41%
UK	48%	44%
Japan	44%	51%
Germany	35%	34%
Brazil	N/A	55%
Canada	38%	44%
Total	43%	47%

Fig 9: Data security lapse in different countries [24]

4. CLOUD COMPUTING SECURITY COUNTERMEASURES

4.1 Counter Steps Proposed by CSA

There are few threats, expressed by cloud security alliance (CSA), which were clarified in the previous section. There are some countermeasures to deal with these hazards.

4.1.1 Defending Invective and Wicked Use of Cloud Computing

To overcome this threat, the registration and validation process must be full proof. Thorough monitoring of network traffic and credit card transactions needs to be done. Users can also analyze public prohibition list for someone's network block.

4.1.2 Defending Malevolent Insiders

One ought to implement strict supply chain management and convey a complete supplier assessment. Also, specify requirement of human resource as part of juridical contract. There should be transparency in data security, compliance reporting and management practices. To deal with this threat users can focus on security break notification technique.

4.1.3 Defending Shared Technology Susceptibilities

Best security practices need to be implemented for installation and configuration of cloud environment. Unauthorized changes and action needs to be monitored. Strong authentication and access control needs to be enforced. Clients can impose service level agreement (SLA) for patching, regular scan for vulnerability and perform consistent audits.

4.1.4 Defending Unprotected Application Programming Interfaces (APIs)

Monitor security model of interfaces provided by cloud supplier. Ensuring robust authentication and access control can be effective during encrypted transmission and understanding the dependency chain related to APIs.

4.1.5 Defending Information Loss

Successful measures are to encrypt and ensures integrity of information in transmission, analyze protection of information during design and run time. Other possible steps to take are to execute strong key generation, management, storage, destruction practices, contractually request suppliers to clean persistent media before it will be discharged into the pool. The supplier backup and retention procedures can also be specified by managers contractually.

4.1.6 Defending Service, Account and Traffic Hijacking

One ought to restrict users from sharing account credentials among them. Users can make use of strong two factor authentication technique as per requirement, and utilize proactive checking to recognize unauthorized activities. An alternate helpful venture to take is to understand security policies of cloud provider and SLAs.

4.2 Counter Steps for Threats from Networking Perspective

4.2.1 Defending Cross Site Scripting (XSS) Attacks

Different approaches like content based data leakage prevention technique, active content filtering and web application vulnerability detection technique have been proposed in [25] to avoid XSS attacks. A blueprint based methodology that minimizes the reliance on web browsers towards recognizing untrusted content over the internet has been proposed in [26].

4.2.2 Defending Sniffer Attacks

Restrict the physical access to the network media such that intruder cannot install a packet sniffer, use encryption mechanism to protect critical information, add MAC address of the gateway permanently to the ARP cache, use IPV6 instead of IPV4 and make use of SSH instead of Telnet, Secure copy (SCP) instead of FTP, SSL for email connections [27]. A sniffing recognition platform in view of ARP (address resolution protocol) and RTT (round trip time) can be utilized to recognize a sniffing framework running on a network [28].

4.2.3 Defending Man in the Middle Attacks

Some essential aspects like separate endpoints, server security methods, accessing software as a service security and assessing virtualization toward the end-point have been carried out to handle with this type of assault in cloud [29]. In most of the cases, the security practices executed in the association's private network also apply to private cloud. Clients need to change network topology in case of public cloud implementation to apply security features [30]. Different tools implementing strong encoding techniques are Dsniff, Ettercap, Cain, Airjack etc., to protect against this type of attack.

4.2.4 Defending SQL Injection Attacks

To check the SQL injection attack users can make use of filtering strategies to disinfect client information. For counteracting SQL injection attacks a proxy based architecture which dynamically identifies and separates client's inputs for suspected SQL control successions has been proposed in [31].

4.2.5 Defending DOS Attacks

Intrusion detection system (IDS) is used for protection against this type of assault [32]. A defense association is used in [33] for protecting against this attack. Separate IDS is used for every cloud. Information exchange is the mode of working for different IDS over network. In the event when a particular cloud is under assault, the supportive IDS alerts the entire system.

4.2.6 Defending DDoS Attacks

R. Gellman [34] had proposed a swarm based logic for defending against DDoS attack. Aman Bakshi in [35] proposed the use of IDS in VM for protecting the cloud from this attack. An intrusion detection mechanism like SNORT is stacked on VM for monitoring both incoming and outgoing traffic [36]. An alternate method is to mount IDS on all physical machines where users VMs are hosted [37]. The performance of this scheme works very well in a Eucalyptus cloud [38].

4.2.7 Defending Domain Name System (DNS) Attacks

Utilizing DNS efforts to establish safety like Domain Name System Security Extensions (DNSSEC) diminishes the impact of DNS intimidations. In the situation when these efforts to establish safety turn out to be deficient when there is some malicious connection in between sender and receiver.

4.2.8 Defending Google Hacking

The end goal to maintain a strategic distance from these hazards is application security ought to be monitored at the different levels of three service delivery models in cloud such as IaaS, PaaS and SaaS as shown in Figure 3. Cloud providers are not aware of the security arrangement organized by client and application management in case of an IaaS model. While

designing an application following points should be considered.

- To protect against the common vulnerability associated with internet there is need to implement standard security measures
- Without testing the authorization and authentication scheme properly applications should not be used
- In case of sudden attack clients can use back up policies like continuous data protection (CDP) to avoid issues related to recovery of data

4.2.9 Defending Security Issues Related to the Hypervisor

If a hacker gets access to the hypervisor he can access any data/code leading to the crashing of the guest OS [21]. Users can establish cloud advance protection system by analyzing the activities of guest VMs as well as intercommunication among the various components by understanding the behavior of different components of hypervisor architecture [39, 40].
In case of KVM [18], since QEMU act as user space program, Linux security modules (LSMs) such as AppArmor or SELinux can be used significantly to diminish the effect of execution of unreasonable code if QEMU is destabilized.

4.2.10 Defending Cookie Poisoning

This can be ensured by performing standard cookie cleanup or executing an encryption plan for cookie information. This can be attained by the scheme proposed in [25]. The acquainted scheme appears to act wisely while dealing with cookie poisoning attack.

4.2.11 Defending Cracking CAPTCHA

Incorporation of numerous authentication procedures alongside identification of CAPTCHA may be a suitable alternative against cracking CAPTCHA. Different techniques such as: actualizing letter cover, variable textual styles of the letters used to plan a CAPTCHA, expanding the string length and utilizing a perturbative foundation can be used to keep intruder away from CAPTCHA breaking [20]. Single frame zero knowledge CAPTCHA outline standards have been proposed, which will be capable to oppose any assault technique of static optical character recognition (OCR).

4.3 Counter Steps for Vulnerabilities in OpenStack Cloud

4.3.1 Defending Heartbleed [23]

Heartbleed can be defended by verifying vulnerability, disrupting users, take the downtime, shut down TSL sessions, update OpenSSL packages, restart all services relaying on OpenSSL, revoke & replace all certificates in use and write a pithy blog post explaining what happened.

4.3.2 Defending ShellShock [23]

ShellShock can be defended by verifying update, verifying vulnerability, notify developers, notify consumers they may be affected and write a pithy blog post explaining what happened.

4.3.3 Defending XEN XSA-108 [23]

XEN XSA-108 can be defended by verifying, testing and applying updates, notify developers, notify consumers they may be affected and write a pithy blog post explaining what happened.

4.3.4 Security Notes [41]

Security related advisories are published from time to time by OpenStack Security Group (OSSG). These advisories may or may not qualify as vulnerabilities. It is intended to raise awareness of security issues that can be mitigated without changing code.
Ex: OSSN-0008 - DoS style attack on noVNC server can lead to service interruption [41].
OSSN-0012 - OpenSSL Heartbleed vulnerability can lead to OpenStack compromise [41].

4.3.5 OpenID Authentication

For authentication purpose platform specific tokens and signatures are supported by OpenStack. One can focus on flexible, decentralized and cloud platform independent authentication mechanism known as OpenID. OpenID is an open-source authentication mechanism in OpenStack cloud environment. It allow a decentralized framework for authentication of users. There are some benefits for web services like improvement in usability and single-sign-on experience for cloud users [42].

5. CONCLUSION

Lot of research is going on to deal with the issues like protection of data, virtualization technique, isolation of resources and network security. Even if there are many advantages of cloud computing environment, there are many problems yet to be sorted. Cloud computing is significant technology not only for internet based services but also for IT field. This paper explored that current security features have many loopholes. The security modules should sort out issues in cloud computing coming from all directions. This article has given security threats of cloud computing and discussed vulnerabilities related to OpenStack cloud. Similarly, it has given some effective countermeasures over each threat/ vulnerability. All the components of a cloud computing environment should be analyzed at both macro and micro level. An integrated solution should be designed in cloud to attract potential consumers.

6. REFERENCES

[1] R. Burnside, 1987. Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies. The Rutgers Computer & Tech. LJ.

[2] David Linthicum, chief technology officer of Blue Mountain Labs, http://www.ebizq.net/blogs/cloudsoa/ 2010/06/top-10-reasons-to-use-and-not-use-cloud-computing.php

[3] N Santos, K Gummadi, R Rodrigues, 2009. Towards Trusted Cloud Computing. In Proc. of the conference on Hot Topics in Cloud Computing, USA.

[4] H Kim, H Lee, W Kim, Y Kim, 2010. A Trust Evaluation Model for QoS Guarantee in Cloud Systems. In Proceedings of the International Journal of Grid and Distributed Computing.

[5] Z Yang, L Qiao, C Liu, C Yang, G Wan, 2010. A Collaborative Trust Model of Firewall-through based on Cloud Computing. In Proceedings of the 14th International Conference on Computer Supported Cooperative Work in Design, China.

[6] M Ahmed, Y Xiang, S Ali, 2010. Above the Trust and Security in Cloud Computing: A Notion towards Innovation. In Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Australia.

[7] Paolo Bonzini, November 12, 2014. http://www.linuxkvm.org/page/Main_Page

[8] Minqi Z, Rong Z, Wei X, Weining Q, Aoying Z, 2010. Security and Privacy in Cloud Computing: A Survey. In Proceedings of the Sixth international conference on Semantics Knowledge and Grid (SKG).

[9] Siani Pearson, 2009. Taking Account of Privacy when Designing Cloud Computing Services. In Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing.

[10] S Ghemawat, H Gobioff, and S. Leung, 2003. The Google file system. In Proceedings of the 19th Symposium on Operating Systems Principles.

[11] Yahoo! Hadoop distributed file system architecture, 2008.http://hadoop.apache.org/common/docs/current/hdfs_design.html

[12] Nida, Pinki, Harsh Dhiman, 2014. A survey on Identity and Access Management in Cloud Computing. In Proceeding of International Journal of Engineering & Technology (IJERT).

[13] T Mather, S Kumaraswamy, S Latif, 2009. Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance. O'Reilly Media, Inc.

[14] Coud Sercurity Alliance, 2010. Top Threats to Cloud Computing.

[15] J Chen, C Guo, 2006. Online detection and prevention of phishing attacks. In Proceedings of the First international conference on communications and networking, China.

[16] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel,and G. Vigna. Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. In Proceedings of the Network and Distributed System.

[17] S Luo, Z Lin, X Chen, Z Yang, J Chen, 2011. Virtualization security for cloud computing services. In Proceedings of the Int. Conference on Cloud and Service Computing.

[18] Paolo Bonzini, https://lwn.net/Articles/619332/

[19] V Ashktorab, Seyed Taghizadeh, 2012. Security threats and countermeasure in cloud computing. In Proceedings of the International journal of application or innovation in engineering and management.

[20] John E. Dunn, 2009. Spammers break Hotmail's CAPTCHA yet again. Tech-world.

[21] J S Reuben, 2007. A Survey on Virtual Machine Security. Seminar of Network Security, Helsinki University of Technology.

[22] G. von Laszewski, J. Diaz, F. Wang, and G. C. Fox, 2012. Comparison of multiple cloud frameworks. In Proceedings of the 5th Int. Conf. on Cloud Computing.

[23] Abu Shohel Ahemad, Ericsson Technology, Robert Clark, HP Technology, 2014. Identifying Security Issues in OpenStack. In Proc. of OpenStack Summit.

[24] Char Sample, Senior Scientist, BBN Technologies, Diana Kelley, Partner, Security Curve. Cloud computing security: Routing and DNS security threats.

[25] D. Gollmann, 2008. Securing Web Applications. Information Security Technical Report.

[26] M Louw, V.N. Venkatakrishnan, 2009. BluePrint: Robust Prevention of Cross-Site scripting attacks for existing browsers. In Proceedings of the 30th IEEE Symposium on Security and Privacy.

[27] Travis Waldo, IT Auditor, NIGC. Information Technology Security: The Changing Threat Environment.

[28] Z Trabelsi, H Rahmani, K Kaouech, M Frikha, 2004. Malicious Sniffing System Detection Platform. In Proceedings of the International Symposium on Applications and the Internet (SAINT'04).

[29] Eric Ogren, 2009. Whitelists SaaS modify traditional security, tackle flaws.

[30] G Singh, A Sharma, M S Lehal, 2011. Security Apprehensions in Different Regions of Cloud Captious Grounds. In Proceedings of the International Journal of Network Security & Its Applications (IJNSA).

[31] A Liu, Yi Yuan, D Wijesekera, and Anglos Stavroun, 2009. SQLProb: A Proxy-based Architecture towards Preventing SQL Injection Attacks. In Proceedings of the SAC.

[32] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, 2010. Intrusion detection techniques for Grid and Cloud Computing Environment. In Proceedings of the IEEE Computer Society.

[33] R Lua and K C Yow, 2011. Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network. In Proceedings of the IEEE Network.

[34] R. Gellman, 2009. Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing.

[35] A Bakshi, Yogesh B., 2010. Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine. In Proceedings of the Second International Conference on Communication Software and networks.

[36] SNORT: An open source intrusion prevention system, https://www.snort.org/

[37] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, 2010. Integrating a Network IDS into an Open Source Cloud Computing Environment. In Proceedings of the Sixth International Conference on Information Assurance and Security, USA.

[38] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, 2009. The Eucalyptus open-source cloud-computing system. In Proceedings of the 9th IEEE/ACM International Symposium on Cluster and Grid computing.

[39] F Lombardi, R Pietro, 2011. Secure Virtualization for Cloud Computing. In Proceedings of the Journal of Network and Computer Applications. Academic Press Ltd. London, UK.

[40] H Wu, Yi Ding, C Winer, Li Yao, 2010. Network Security for Virtual Machines in Cloud Computing. In Proceedings of the 5th Int'l Conference on Computer Sciences and Convergence Information Technology, Seoul.

[41] Security Notes by OpenStack Security Group (OSSG), https://wiki.openstack.org/wiki/Security_Notes.

[42] R Khan, J Ylitalo, A Ahmed, 2011. OpenID Authentication As A Service in OpenStack. In Proceedings of the 7th International Conference on Information Assurance and Security.