TAXONOMY OF CLOUD SECURITY

Sanchika Gupta, Padam Kumar

Department of Computer Engineering
Indian Institute of Technology Roorkee, Roorkee Uttarakhand-247667

ABSTRACT

Cloud computing is envisioned as the next generation architecture for IT Enterprises, and has proliferated itself due to the advantages it provides.Cloud computing provides solutions for carrying out efficient, scalable and low cost computing. The pay per usage concept of Cloud computing increases the resource utilisation of a vendor's computing power and resources; at the same time,it results in reduced hardware costs forits users. It also provides access mobility, easier maintenance, scalabilityand operability in terms of its management and usage. Because of the facilities and solutions it provides to the industry for the next generation computing, it is vulnerable to a variety of known and unknown attacks from attackers.Hence, securinga Cloud environment is a critical problem that needs urgent attention.This articlefocuses on a taxonomy of possible attacks on a Cloud environment and a taxonomy of the defence .The attack taxonomy describes existing threats on Cloud security, and the defence taxonomy gives a classification of the various counter measures that can be taken to protect the Cloud environment from such attacks. The aim of this article is to provideresearchers, academicians and industry with a better understanding of existing attacks and defence mechanisms on Cloud security.This is to provide a clearvision of the challenges that should be worked onto ensure next generation security forCloud computing.

KEYWORDS

Cloud, security, attack, defence, Taxonomy, Intrusion, Detection

1. INTRODUCTION

The Internet has been a driving force towards various technologies that haveemerged, and it has changed the way the computing world is looked at (Gupta S. Communications in Computer and Information Science et.al 2012). One of the latest, emerging internet-based technologies is Cloud computing (Goscinski A.) (Buyya R. et al 2009).Itis undergoing an imperative success with almost all the big names trying to make an entry into it. The list includes Amazon, Google, Rack space etc. The concept of renting resources on a pay per usage model was previously used by renowned telecommunication companies with heavy operational resources. In such cases, they rentedout their additional resources to smaller telecommunication companies(Buyya R. et al.2009).This technique of renting out spare resources helped them to earn more and utilise their resources optimally and efficiently. Presently, for IT Enterprises, Cloud computing is an online (network access-based) form of computing wherein users can access services such as Storage, Computing, Applications etc.via well-known basic interfaces such asbrowser. According to the US National Institute of Standards and Technology (NIST), Cloud computing is a model that provides ubiquitous and demand-based access to a shared pool of resources that are configurable (S. Gupta et al. 2013). As well, they can be provisioned, managed and released with minimum management efforts or Cloud service provider interaction. The resources include Network, Storage, Applications and Computing power and they are provided on an on-demand network access model (Brown E. 2012). In summary, NIST has captured five essential Cloud

DOI : 10.5121/ijcsea.2013.3505

characteristics which are: on-demand self-service, ubiquitous network access, resource pooling, rapid elasticity and measured service(Computer Security Division 2007).A Cloud is provided with three Service Models: SaaS, PaaS, and IaaS.

SaaS provides the ability to Cloud users to access Applications running on a Cloud Infrastructure. Such access to hosted applications is provided with the use of thin client interfaces such as Web browsers or with program interfaces. PaaS provides to its users the capability of deploying user created or acquired applications using programming facilities, such as tools, libraries and services provided by the service provider. IaaS provides to its users the capability of provisioning a network, storage and fundamental computing resources so that they can deploy and run arbitrary software over it. One should understand that it is not only distributed computing given a new name but; rather, it is a new form of computing with new concepts and paradigms. These are such as virtualisation technologies that try to optimise resource usage by dividing a single physical infrastructure into many virtual infrastructures. These infrastructures are individually separated and are custom built for a specific purpose on demand(Dhage S.N and Meshram B.B. 2012). Based on the service it provides, a Cloud is categorised into two types: (a) Compute Clouds that provide computing power as a service, and (b) Data Clouds that provide data storage as a service to their its users.

Based on the type of access to it, a Cloud can be designated asa PublicCloud, Private Cloudor a Hybrid Cloud. All of the Clouds mainly provide three facilities to their users; these are Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS). The advantages of using Cloud computing as from various studies from researchersincludes but are not limited to: a) Reduced hardware costs, b) Mobility of access around the globe, c) Easier maintenance, d) Computing flexibility, e) Use of shared resources, and f) Highly automated.But, these advantages could indeed be at stake because of concerns about the risks and threats related to the potential misuse of the Cloud computing model. In fact, the extent of the availability of the resources acts as a catalyst to distributed attacks on confidential data(Mazzariello C. et al. 2010). Cloud services and their distributed nature make Cloud computing highly vulnerable to the risk of distributed attacks. It is alsovulnerable to theattacks arising from vulnerabilities existing in the underlying technologies used for deploying Clouds, such as virtualisation technologies. The security of the data, infrastructure, applications and network are the major considerations in Cloud security. Attacks, such as Denial of Service (DOS), cross site scripting, network penetration etc. are more common in the case of Cloud computing. This is because it renders the services of the Cloud unusable and causeshuge losses for both the service provider and their clients(Kwon H. et.al 2011).

Security is the most important factor that has majorly affected the growth of Cloud computing in the past few years (Gupta S. et al. Computational Aspects of Social Networks (CASoN) 2012) (Subashini S and Kavitha V). A very recent example is the Go Grid security breach (in August, 2012). In this case, an unauthorised third party tried to view the account information along with the payment card data of the customers. Another is the Drop box (a well-known Cloud file sharing facility)getting hacked in July, 2012. The online file storage service was compromised and usernames and passwords were stolen by third party websites.This information was then used to access the Drop box accounts of the users. Another is the Azure leap year bug which took place on Feb. 29, 2012. In this case, Microsoft's Azure Cloud infrastructure and development service experienced a serious worldwide outage which led to Hotmail, SkyDrive, MSN, Azure and Office 365 going down for a couple of hours. Twitter also experienced an outage in June, 2012 for more than an hour. Another is the breach of Sony’s PlayStation network which took

place on May 13th, 2011; it has been recorded as the second-largest online data breach in the U.S. historyanother instance of a Cloud attack is recorded on the Amazon EC2 cloud, which took place in October, 2009; it rendered Bit Bucket's servers down for 19 hours. Bit bucket rents its computing infrastructure from Amazon(Metz C. 2009). In 2011, researchers identified three different ways of hacking Drop box. In June, a flawed update on the site made all _user accounts open to be accessed by anyone who typed in an email address associated with that user'sDropbox account. A breach over Epsilon (a well-known email marketing company) in 2011,leaked millions of names and email addresses from its customer database. At the end of that year, Stratfor, a company that provides a subscription-based geopolitical analysis service, saw its servers breached by a malicious entity.Figure1 shows a clear description of the various Cloud security attacks over the years. Since Cloud computing security is identified as a major problem by industry, researches are ongoing to devise techniques that can handle the situation. However, there exists nowhere,a detailed description of Cloud attacks and defence mechanisms that can help academia, industry and researchers to getter a deeper insightintothe attacks so that the associated vulnerabilities can be identified and removed(Vieira K. et al. 2009). This article explains various attacks and defence mechanisms for securing Cloud computing.Italso provides an exhaustive comparison of the various existing techniques to detect and countermeasure the attacks in the Cloud computing environment.

In this article, on the basis of the current threat scenario of Cloud and with the use of threat modelling techniques, the well-known attacks on the Cloud environment are identified. The attacks have beenidentified based on the threat analysis over the service layers provided by Cloud Computing. The attacks originating from the identified threats are listed in the paper to provide a clear vision towards possible and ongoing attacks over Cloud. The location of the security attacks and the layer on which the security attacks are targeted are also explained in detail. The paper also identifies the defence measures for ensuring security from the identified attackson the Cloud environment. The focus is on the fact that if these attacks can be analysed for a Cloud deployment and effectively taken care of by applying the respective defence measures, the Cloud environment can be secured from the attacks. These attackscantake one or morecombinations of well-known attacks as its ingredients to launch massive and planned attacks.The article is divided into 4sections. Section 2 provides the taxonomy of Cloud attacks with section 3 providing a description of defence mechanisms that can be used for their countermeasure. Finally, section 4 ends this article with the conclusions.

2. TAXONOMY OF CLOUD SECURITY ATTACKS

While there are many threats over the Cloud environment, we have categorised well-known threats into the categories given below (Los R. et al. 2012):

1. **Abuse of Cloud Computing resources:** Many companies give access to Cloud resources on a trial basis. Researchers have found that such anonymous and normal registration processes are used by malicious users to use Cloud computing resources for carrying out unwanted activities. Cybercriminals obtain better immunity by doing their malicious activities in the shade of a Cloud computing environment. Presently, the mostly affected service layer is PaaS but with time, this will attack the IaaS platform as well. The basic attacks that are launched over Clouds for carrying out such abuses may include password cracking, Denial and distributed denial of attacks, botnet monitoring and control, and malicious data hosting. Examples of such abuses are in the industry where malicious entities have hosted Botnets,

Trojan horses and malwares (Danchev D. 2009) on IaaS infrastructures. Such activities have led to an extent where the block of the network addresses of IaaS is blacklisted.

2. **Interface Insecurity:** Cloud is service oriented architecture. A user uses these interfaces to interact with Cloud services. All of the provisioning and management work over a Cloud is managed and performed by these API's; hence, Cloud security and availability rely on the security of these API's. Therefore, if these API's are vulnerable or tampered with maliciously, they can allow outside entities to circumvent the defined policies of usage and working in the Cloud. The basic attacks for such kinds of threats come from the vulnerabilities arising from improper authorisations, clear text transmission of content, and the limited availability of logging capabilities and unknown API dependencies. Hence, to remove such threats, it will require a well analysed security model with enhanced access control, authentication mechanism and encrypted data transmission. One should also check, understand and analyse external dependencies on the API's and how they can affect the environment in terms of security. These attacks affect all three layers of the Cloud.
3. **Issue related with Shared Technology:** Hypervisor is utilized for providing virtual access to physical computing resources. It provides a guest operating system to have access to virtualized physical resources. But well-known attacks over virtualization platforms, such as VM Escape, VM Hoping etc., have proved that these platforms are not safe. Moreover, the concept of the data isolation of the individual Cloud users does not have a sure implementation in the Cloud environment. Hence, it is a requirement that security models and implementations should be devised and must be taken into practice. This is so that a user does not have access to another user's personal data and resources, such as network traffic etc. Further, a user will not interrupt the operation and availability of services of other tenants. To remove such attacks, it requires that the system must be monitored for unauthorised changes and modifications, vulnerability scanning, patching and configuration audits. This kind of threat generally hits the IaaS layer of the Cloud infrastructure.
4. **Data Loss and Leakage:** Data loss in Cloud can happen in many ways. Some include deleting records, unlinking a record, destroying the encoding keys etc. All of these may lead to the loss of data. The condition becomes adverse if the data loss happens with prioritized Cloud users who are using the facility for data storage. Also, there is a need for data leakage security to be implemented so that important and secret data will not go into the wrong hands. The problem is severe because of the amount of data access operations and the kind of data information stored on Clouds. To reduce the risk from such a threat, it requires that good access control to be taken into practice with data flow remaining encrypted and its integrity being verified. Also, data must be stored securely and integrity monitoring periodically taken into practice. This threat generally acts as a risk over all of the service layers in Cloud.

Some of the other identified threats in past researches by academia and industry on Cloud include Malicious Insiders, Service Interruption through hijacking(McMillan R., 2009) and unknown risk profiles. However, the threats resulting in known Cloud attacks are from one of these four Threats explained over Cloud in Perilli A. et al. Based on the analysis of the threat scenario of Cloud that identifies various well-known attacks and countermeasures along with our analysis of the threats over Cloud on the basis of the Cloud service layer and the location of the security attacks a taxonomy attacks has been created.Figure1provides thistaxonomy of Cloud security attacks enlisting existing potential threats to Cloud security. The classification has been performed based on various attack primitives. Each of the attack types is described based on the way it initialises, propagates and affects the victim.

We have classified existing and potential attacks on Cloud into categories based on certain parameters shown in Figure 2. They are described in the next section. The attacks have been individually analysed for determining specific vulnerabilities that are responsible for threats. Notations used in the classification with their short description are as follows: - LS: Location of Security, IA: Information Assurance, UA: Unauthorised Access, AR: Access Rights, CL: Cloud Layer, CI: Code Instability, VT: Victim Type, EV: Exploitation of Vulnerability, FP: Fault Propagation, VM: Virtual Machine, HR: Hypervisor Risk, IM: Invalid Modification.

2.1 LS: Classification by Location of security attack

2.1.1 LS-1: Security Attack at the Cloud Service User's End:

LS-1: IA: Classification by information assurance: Information Assurance is one of the key characteristics expected from a Cloud by its users. But there are various threats and risks over the Cloud that led to attacks that hamper the information assurance characteristic of Cloud. The attacks on the various prerequisite qualities for ensuring information assurance to Cloud users are as follows:

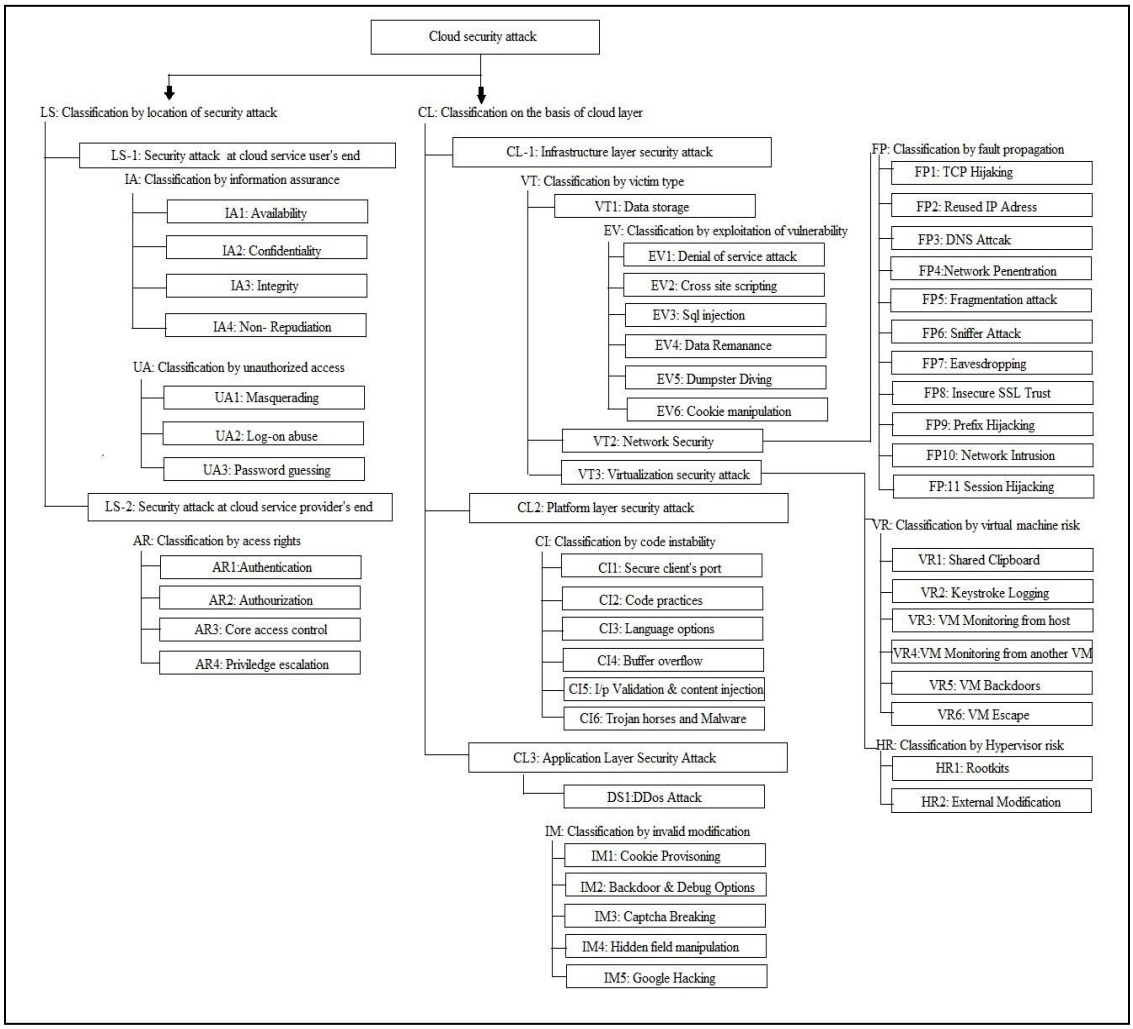

Figure1. Taxonomy of Cloud attack

LS-1: IA1: Availability: By Availability in Cloud from a user's perspective, we mean the availability of the resources requested by a user. They can be computing or networking or data storage resources. Attacks on availability in Clouds are mostly Denial of service attacks on networks and computing infrastructures. Availability attacks in Cloud-based systems focus on attacking a specific part of the network or computing resources with a huge number of unwanted computations or network queries and responses; For example, DDOS attacks.

LS-1: IA2: Confidentiality: The attacks on confidentiality attempt to gather secret information travelling onto the Cloud by intercepting the network channel of the Cloud network. For example, if a shared bridge is intercepted, then it will reveal the data of all the VMs using the same bridge. It will become worse if the data is going in unencrypted format. Different types of attacks on confidentiality in Cloud include eavesdropping on data from neighbouring or remote VMs, decrypting the key and man in the middle attacks.

LS-1: IA3: Integrity: The idea behind attacks on integrity is to modify the important data and configuration files which are responsible for the configuration, management and/or proper functioning of the Cloud. This attack on Cloud will result in malicious configurations or monitoring of information which is available to the Cloud manager. As we know, in Cloud platforms, such as open nebula which monitors a VM periodically and provides the log information to the central Cloud manager, if the Integrity of the logs is not maintained it will result in an attack being undetected. Also, if the configuration information travelling from Cloud to a client VM is modified, it will also cause the unstable and improper configuration of the client VMs. Both scenarios are always possible in a real time cloud environment.

LS-1: IA4: Non-repudiation: A repudiation attack on a Cloud system is because of the unavailability of specific controls and facilities to properly track and log user's actions. This allows malicious operations from intended users, also called nefarious users, with the system having no backtracking mechanisms to take action against them. Such weakness in the system can be used by Cloud users to launch planned attacks with the user of massive Cloud resources on Cloud itself. For example, a Cloud user can launch DDoS attacks to another client VM, Cloud infrastructure or the outside world if proper tracing and logging mechanisms are not available for non-repudiation.

LS-1: UA: Classification by unauthorised access

LS-1: UA-1: Masquerading: Masquerading attacks, as known in the context of information security, are a type of attack in which a malicious userillegitimately obtainsthe identity of some known privileged user so as to gain access to system resources to which the illegitimate user's access was previously restricted. In Cloud, the threat of such an attack is immense. This is because there areconfidential data on the Cloud systems of various users. If masquerading attacks are launched over a Cloud, it will create an immediate risk by compromising the data of the Cloud users. This is because any nefarious user will be able to provide his/her identity as a different user to the Cloud authorisation mechanisms resulting in unauthorised access to the shared Cloud resources and data of other users. This will be a massive attack if he/she can masquerade as a Cloud admin., hence getting control of all security policies and operations that can be subverted for bypassing detection.

LS-1: UA-2: Log-on abuse: Log-on abuse can be defined as, legitimate users accessing dataor services of a higher security level on a Cloud system that are not intended to be used by them. This type of abuse focuses primarily on those users who might be legitimate users of a different system or users who have a lower security classification(Krutz R.L. and Vines R.D., 2009)., This attack over Cloud is launched by Malicious Insiders. The escalation of privileges by a nefarious user to higher security levels, such as Cloud admin., for malicious purposes is an example of this type of attack.

LS-1: UA-3: Password guessing: This is a passive attack in which an attacker gains access to a person's privileged authentication information by password guessing and othermeans. Theseinclude guessing, looking for notes on the victim's system, eavesdropping on the network to get access to unencrypted passwords, and gaining access to a central database where all the passwords are stored. Others are checking social websites to know about the personal details of the victim like date or place of birth, favourite animal, sport etc. The technique of dumpster diving is a well-known technique utilised by attackers for carrying out this attack. General authentication information, such as usernames and passwords, are the most commonly used mechanism to authenticate users to a Cloud system. Therefore, obtaining passwords is a common and effective attack approach to gain access to an authorised Cloud user account. In this way, theycan perform abuses on or with Cloud resources using the wrong identity(Krutz R.L. and Vines R.D., 2010). This attack exists since backbut its severity has increased because of the shared data and resources existing in the Cloud environment. Hence, such attacks subvert Cloud as a whole.

2.1.2 LS-2: Security attacks at Cloud service provider's end:

LS-2: AR: Classification by access rights: Different users in a Cloud have different access rights or privileges which are dependentupon the trust levels and the kind of services they have subscribed for. For example, normal users can be granted different access rights from one service to another based on the trust the system has on their operations. While administrators have full access control over all data in the system because their profiles are more trustworthy to the system as compared to the user. Attacks that target Cloud environments through attacks on subverting access control systems are as follows:

LS-2: AR1: Authentication: Authentication plays a critical role in the security of Cloud applications. When a user provides his login name and password for authentication, the Cloud application assigns to the user specific privileges to use the system and Cloud resources based on the identity or trust level established by the credentials supplied earlier.

The authentication protocols operate over the Hypertext Transfer Protocol or Secure Socket Layer (SSL)/ Transport layer security (TLS) with the user credentials enclosed in the request/response traffic. Hence, such credentials can always be obtained from Cloud users through sniffing or advanced and well-known web and email based attacks such as Phishing. There is a need for stronger authentication schemes or two factor authentication schemes so that the authentication measures in Cloud can be made stiffer and more fault tolerant to attacks such as Phishing. Also, Phishing solutions can be added to Cloud as utility or bowser applications as well.

LS-2: AR2: Authorisation: In a Cloud system on the service provider's end, authorisation attacks in clued the attacks over the Cloud service provider mechanism for determining if a Cloud user, Cloud service, or Cloud application has the required permission to perform a requested action. For example, many Cloud facilities, such as shared web servers, allow certain registered

users to access specific content or functionality based on their credentials and level of trust. They should not be allowed to use other resources to which access is restricted. Using various techniques, an attacker can fool a web site into increasing their privileges in order togetauthorisation to access confidential data and resources in the Cloud. One of these techniques is(Cyber security and Communications at US Dept. of Homeland Security, 2012):Credential/Session prediction, which is a method of hijacking or imitating a Cloud application user.Other targeted attacks include SQL injection.

LS-2: AR3: Core Access controls: The virtual machine's hypervisor facilitates hardware virtualisation that mediates all hardware access for running virtual machines. The hypervisor which provides simultaneous access to various guest operating systems is exposed to security threats. It can endanger the trusted network through poorly designed access control systems, deficient patching and lack of monitoring (Krutz R.L. and Vines R.D., 2010). Many of the hypervisor layer's vulnerabilities can result in privilege escalation attacks. These can be utilised by well-known kits, including black hole, for compromising the access control systems.

LS-2: AR4: Privilege Escalation: Specific privilege escalation attacks at the Cloud service provider are network intrusions that take advantage of programming errors or design weaknesses. This is to grant the attacker unauthorised access to the Cloud network and its associated data and services. There are two types of privilege escalation attacks: vertical and horizontal. In a vertical privilege escalation, an attacker is granted higher privileges than he/she is supposed to have. This is fulfilled by performing kernel-level operations that allow the attacker to run unauthorised codes. In horizontal privilege escalation, an attacker uses the same level of privileges he/she has already been granted but using the identity of another user with similar privileges.

2.2 CL: Classification of attacks on the basis of Cloud service layers:

2.2.1 CL-1: Infrastructure layer security attack: The infrastructure layer (IaaS) provides infrastructure services such as data storage and computing in Cloud. It provides user's the space for deploying their custom platforms and software services. Various attacks identified and classified on the infrastructure layer of Cloud are classified as follows:

CL-1: VT: Classification by victim type: Based on the part of the Cloud infrastructure (storage, network and virtualisation)which is the victim of an attack, attacks are classified into data storage attacks, network security attacks and virtualisation security attacks

.

CL-1: VT-1: Data storage: There are various service providers in the market who provide Storage-as-a-service (an offering from IaaS). To secure the data placed in the Cloud, these service providers adopt different security mechanisms. We have identified and classified the attacks over the data storage on Cloud as follows:

CL-1: VT-1: EV: Classification by exploitation of Vulnerability: On the basis of vulnerabilities exploited for carrying out an attack on Cloud storage, the classification is as follows:

CL-1: VT-1: EV-1: Denial of service Attack (DoS): Denial of service attacks onCloud storageintends to prevent the usage of Cloud data storage resources. E.g., the attacker may display an offensive message on the victim's interface periodically after every "t" seconds or append unnecessary statements to every file on the disk hence, tampering with them. Other than that, anattacker may consume every free space on the victim's disk, leaving no space for the victim to

save the files he/she has been editing. DoS attacks cause loss of service, which is the inability of a particular service to provide its functionalities in a normal way to its users, or it can be described as the temporary loss of availability of a network's connectivity and services(Cyber security and Communications at US Dept. of Homeland Security, 2013).DDoS attacks generally exploit un-patched vulnerabilities in underlying operating systems, network protocols etc.(Reiher P. and Mirkovic M, 2004).DDoS attacks severely disrupt cloud storage services and make them unusable to Cloud users which also result in decreased trust onCloud services.

CL-1: VT-1: EV-2: Cross-site scripting (XSS): Cross-site Scripting (XSS or CSS) is an attack technique that forces a web site hosted on the infrastructure layer to emulate an attacker-supplied executable code, which loads itself into a Cloud user's browser. This kind of attack takes advantage of a web site vulnerability in which the website displays content that includes un-sanitised user-provided data. For example, to propagate this attack, an attacker can place a malicious hyperlink, which consists of an intrusive code, by breaking into (through XSS) an online social networking website or shopping webpage. The users who then select that hyperlink will get affected through the malicious code.

CL-1: VT-1: EV-3: SQL injection: The SQL injection is a technique used by attackers in which malicious SQL queries are inserted into the web hosted by the infrastructure layer in a Cloud system. Attackers, generally Cloud insiders and skilled attackers, take advantage of the fact that programmers often chain together SQL commands with user-provided parameters. Hence, there is a possibility of embedding SQL commands inside these parameters to perform malicious activities, such as getting access to Cloud resources through user account break-ins. The result is that the attacker can execute arbitrary SQL queries and/or commands on the backend database server through the web application interfaces without having authorisation to do so.

CL-1: VT-1: EV-4: Data Remanence: Data Remanence is a term used for the residual representation of data that remains when the data is removed or deleted. This residue may result due to various operations like the file deletion operation, reformatting of storage devices etc. This is because that after these operations is performed, previously written data remains intact. Data Remanence may lead to the disclosure of confidential information. In Cloud, the effects of Data Remanence are more complicated because you do not know exactly where your data has been placed. The Cloud service provider provides you with storage at different physical location. Removing data from that location means reallocating those sectors to other instances. Until those locations are rewritten from the data of other instances (probably from some different user) the previous data remains intact.Hence, an enterprising hacker might be able to read your data by looking at the bits in their newly provisioned instance.

CL-1: VT-1: EV-5: Dumpster Diving: Dumpster Diving can be defined as the process of diving for information from data that is declared as waste. It can also be described as the method for recovery of information that is discarded by a Cloud user or Cloud service provider. In many cases, information found in trash can be very valuable to an attacker as it can be a targeted dive looking for a specific user's data shared in Cloud. Discarded information may include technical manuals, passwords, telephone directories, credit card numbers, and organisational growth charts.

CL-1: VT-1: EV-6: Cookie manipulation: Cookie manipulation, as the name signifies, is an attack which is launched by manipulating the cookies stored by the browser. This can be easily launched by nefarious Cloud insiders or Cloud admin. This will help them launch specific attacks, such as Phishing on Clients, or subversions to Cloud authentication measures. This is accomplished by inserting a custom HTTP header or by infusing a META tag. Attackers

normally alter cookie values to authenticate themselves on a Cloud interface in an unauthorised manner.

CL-1: VT-2: Network security attack: The identified and analysedNetwork level security threats over Cloud are as follows:

CL-1: VT-2: FP: Classification by fault propagation: On the basis of the manner in which a fault is propagated, the attacks onthe Cloud network can be classified as follows:

CL-1: VT-2: FP-1: TCP hijacking: In this type of attack, an attacker steals or hijacks a session between a trusted client VM and the Cloudmanager. TCP hijacking can be describedas the spoofing of the TCP packets to disconnect the authorised Cloud user from his/her ongoing authentic connection with the Cloud remote server. The attacking computer substitutes its IP address for that of the trusted client and also mimics the correctly sequenced spoofed TCP packets, and the server continues the dialog believing it is still communicating with the trusted client(Cyber security and Communications at US Dept. of Homeland Security, 2013).

CL-1: VT-2: FP-2: Reused IP addresses: As the nodes of a network are provided with an IP address, the IP address is basically a discrete quantity. In a Cloud's dynamic provisioning of network resources, the IP address associated with a Cloud user is assigned to a new user when the old user moves out of a network. This sometimes creates risks to the security of the new user. This is because there is a noticeable time lag between the change of an associated IP address in DNS and the clearing of that address in the caches of the DNS entries. Sometimes, however, the old IP address is assigned to a new user; however, one cannot neglect the chances that some other user will access the data associated with the sessions of the old IP the address stills resides in the DNS caches.

CL-1: VT-2: FP-3: DNS attacks: A Domain Name Server (DNS) attack takes place when malicious data is placed in the DNS database from sources which are not authoritative in Cloud. DNS 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(Kavitha V. and Subhasini S., 2011). But, nefarious users or Cloud insiders can use their privileges to enable the changing of the internal mapping. This results in the naïve Cloud users getting redirected to malicious locations toget access to resources. For example, the manipulation of DNS entries can lead to Web Phishing attacks on Cloud users resulting in the loss of the user's credentials and authentication information.

CL-1: VT-2: FP-4: Network penetration: Network penetration is an attack on Cloud in which the attacker tries to penetrate the Cloud network infrastructure by evading the network security measures through advanced network evasion techniques. Some of the techniques include port scanning on Cloud data centers and central manager components. This technique looks for specific open ports and gathers information about the system so that more specific network attacks can be launched. Some of the possible and ongoing attacks in this category include: IP Random Options, SMB Session Mixing, TCP Urgent Pointer, MSRPC Object Reference etc.

CL-1: VT-2: FP-5: Fragmentation attack: IP fragmentation is the process of breaking down a single IP datagram into smaller packets to be transmitted to different locations. IP fragmentation attacks use various IP datagram fragmentations to disguise their TCP packets from a target's IP filtering devices(Cyber security and Communications at US Dept. of Homeland Security, 2013).[30]. The following are two examples of these types of attacks: A *tiny fragment attack*

occurs when the attacker inserts a very small fragment into the TCP header that forces the TCP header field into a second fragment. If the target's filtering device does not enforce a minimum fragment size, this illegal packet can then be passed on through the target's network. An *overlapping fragment attack* is another variation on a datagram's zero-offset modification. In this, the re-assembled packet starts in the middle of another packet. As these invalid packets are received by the operating system, they are allocated memory. This uses all the memory resources in a virtual system and renders the machine unusable. These attacks also are in existing systems but the focus of them in the Cloud environment. This is because these attacks need to be taken care of because of the immense impact they can have because of Cloud's distributed nature.

CL-1: VT-2: FP-6: Sniffer attack: Sniffers are network packet analysers. These tools are used for capturing important information travelling on the Cloud network by malicious Cloud users or insiders for their malicious purposes. These types of attacks are launched by Cloud user or malicious insiders using applications that can analyse the traffic flowing through the network. They can, in turn, capture and save them. One of the well-known network sniffers that are applied to both a simple network configuration and a distributed environment, such as Cloud, is Wire shark. The worse thing can happen if it is being transmitted in plaintext. In this case, the sensitive information of all other Cloud users can be captured by a Cloud Manager or a nefarious Cloud user. 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 Cloud network for preventing such attacks(Kavitha V. and Subhasini S., 2011).

CL-1: VT-2: FP-7: Eavesdropping: There are three kinds of eavesdropping attacks on Cloud: Traffic analysis of the client VMs, passive eavesdropping and active eavesdropping on data inside the Cloud network. **Traffic Analysis**: Traffic analysis is a technique in which a nefarious Cloud user or insideranalyses the Cloud's internal or external network and extracts the information about the VM network. This helps in gathering the network statistics of a specific client VM or Cloud as a whole to launch more sophisticated network attacks over them. **Passive Eavesdropping**: With this type of attack, the attacker simply monitors the traffic traversing the Cloud network. The attackermay store it for further analysis, at a later time, for information from a specific client VM. **Active Eavesdropping**: In this type of attack, the attacker can either modify a packet being transmitted or inject a new packet into the Cloud network to disrupt the configuration or monitoring mechanisms with others in the Cloud environment. Sometimes, the goal of the attacker is to prevent the authentic packet from reaching its authentic destination. One of the methods for accomplishing this is to modify a packet's destination IP address in transit.

CL-1: VT-2: FP-8: Insecure SSL trust: There are some serious flaws found in the SSL protocol used for secure communication on the internet. The attack, if it occurs on Cloud, will allow the attackers to compromise the secure traffic between the websites and browsers of various Cloud users. These attacks enable sophisticated Cloud users and insiders to steal passwords, hijack online banking sessions etc.

CL-1: VT-2: FP-9: Prefix Hijacking: Prefix Hijacking is a network attack on a Cloud infrastructure that gives malicious parties access to untraceable IP addresses. It occurs when a malicious autonomous system announces to its peer autonomous systems that a block of IP addresses belongs to it, when the case is that it does not.

CL-1: VT-2: FP-10: Network Intrusion: Network intrusion is a basic attack which refers to the unauthorised entry into the system by attackers or Cloud insiders through the exploitation of the

network vulnerabilities existing in the system. Unlike a logon abuse attack, in this case the intruders can be external to the system, i.e., they may or may not bea part of the system. It is also known as a network penetration attack, as it exploits known network security vulnerabilities in a Cloud system forintrusion purposes. We will not focus more on it as this is a well-known attack on networksalthough, it does have major impacts on Cloud.

CL-1: VT-2: FP-11: Session hijacking: Session hijacking is a sophisticated attack on the Web these days that allows an attacker to take control of the validated and authenticated session of a user. In this case, a Cloud user may find his/her session no longer available but will not know the reason behind it. This is a specific kind of attack that occurs while the original user's session is active but the attack continues a long time after the user leaves the network. There are two steps to complete a successful session hijacking attack which are as follows. In the first step, there must exist some manner that an attacker can determine and use to represent him as the user to the network from which he will try to obtain the control of the session. This is generally performed by using a technique for eavesdropping on the data of the user to gain access to the information, such as the kind of encryption mechanism used etc. In the second step, the attacker applies some techniques so that the user must stop his/heron-going session. The attacker can use well-known techniques, such as the man in the middle attack. Hence, the attacker can issue various kinds of intermediate messages to the user so that he/she will give up the session.

CL-1: VT-3: Virtualisation security attack: This categorisation is for a new type of attack because of the vulnerabilities in the virtualisation platforms that act as a base for the Cloud environment. Virtualisation attacks are a type of infrastructure layer security attack that is classified on the basis of virtual machine risks and hypervisor risks(Kavitha V. and Subhasini S., 2011).The analysis of these attacks and their classification is as follows:

CL-1: VT-3: VR: Classification by virtual machine risks: Security threats in virtualisation platforms are from the internal and external interfaces of Cloud. We have classified the attacks based on the security risk that they create on virtual machines.

CL-1: VT-3: VR-1: Shared clipboard: Shared clipboard is a feature that allows the sharing of the buffer between Virtual Machines and hosts. These facilities include copy and paste operations with the use of buffers between VMs and hosts. If such functionality is allowed without proper configuration, or if the shared clipboard is available to nefarious users by some means, then it allows them to read the common buffer resulting in a compromise of data shared between other VM's and /or central hosts. Hence, it creates risk over virtual machine data integrity and security, and needs to be taken care of.

CL-1: VT-3: VR-2: Keystroke logging: Keystroke logging is the concept of tracking and logging the keys from the keyboard of an interface, in a manner such that the victim using the keyboard remains unaware of being monitored. This technique of logging user typed keys will help in obtaining user personal, financial and transactional information. Such keystroke loggers can be installed by malicious Cloud insiders with sufficient privileges to do so and hence, can compromise the security of a Cloud user. The key logger can also reside in a hypervisor running underneath the host operating system, which remains untouched. Hence, detectors for identifying keystroke loggers at Client VMs and Cloud hosts or at hypervisors need to be taken into consideration.

CL-1: VT-3: VR-3: VM monitoring from the host: This attack allows the host to control operations, such as the starting, pausing and restarting of VMs. It also allows the monitoring and

configuration of VM resources, such as CPU, Memory, disk, and the VM's network usage. Some other operations, such as the adjustment of the number of CPUs, amounts of memory allocated and the number of interfaces that are available to a VM, are also allowed. This is when these privileges are not provided to the hosts as per user agreement.

CL-1: VT-3: VR-4: VM monitoring from another VM: Since virtual machines run on a subset of hardware resources or on shared resources, the resource usage of a VM can be observed from outside the VM. If the VM platform uses a virtual hub or switch to connect the VMs to the host, then intruders may use ARP poisoning to redirect packets going to or from other VMs. Hence, this creates risk to Cloud user data and service monitoring by malicious users.

CL-1: VT-3: VR-5: VM backdoors: A backdoor attack is a way of getting access to the Cloud system by bypassing normal authentication steps. A backdoor is a covert communication channel, between the guestoperating system and the host. Further, it could allow attackers to perform potentially dangerous operations and needs to be taken care of.

CL-1: VT-3: VR-6: VM Escape: A virtual machine escape is an attack in which an attacker runs a specific code on the virtual machine that allows the host operating system to break out and interact with the hypervisor. Such an attack would give an attacker complete access to the host operating system and all the virtual machines. This would eventually result in a complete failure of the security mechanisms of the Cloud system.

CL-1: VT-3: HR: Classification by hypervisor risks: Based on the threats on the hypervisor in Cloud, we have identified and classified attacks on the hypervisor in the virtualisation environment which are as follows.

CL-1: VT-3: HR-1: VM Root kits Hypervisor is a part of a virtualisation environment that handles the virtualisation of physical resources, allows host resource sharing and enables VM/host isolation. The hypervisor is susceptible to risk from known vulnerabilities. The risk increases proportionally to the volume and complexity of the application code. VM-based root kits can remain hidden from normal malware detection systems by attacking onhypervisor and creating a cover channel to dump unauthorized codes into the system [Martinez C.A., Echeverri G.I. and Sanz A.G.C., 2010].

CL-1: VT-3: HR-1: External Modification to the hypervisor: A self-protected virtual machine may allow direct modification of its hypervisor by an external intruder. This can occur in a virtualised system that does not validate the hypervisor integrity as a regular process.

2.2.2 CL-2: Platform layer security attack: The platform layer is the second service layer ofa Cloud environment which provides Platform as a Service (PaaS). The various attacks possible on the platform layer of a Cloud are classified as follows:

CL-2: CI: Classification by code instabilities: The classification of security attacks on the platform layer because of the instabilities in the code are as follows:

CL-2: CI-1: Secure client's port: The open client's port to the Cloud might provide an attack path if it is not properly provisioned with security measures. Therefore, the client needs assurance that the computations and data exchanges are conducted in a secure environment. This assurance is affected by the trust enabled by cryptographic methods.

CL-2: CI-2: Code practices: The information provided in a Cloud server code may pose a risk to privacy and confidentiality. So, to prevent the sensitive information from being exposed to the attacker, appropriate measures should be taken into consideration. An attacker may spend hours examining HTML scripts for information that can be used to find a way to intrude based on the vulnerability detected. Hence, the lack of secure code practices in Cloud may lead to various attacks due to the exploitation of code vulnerabilities by attackers.

CL-2: CI-3: Language options: In Cloud server applications, languages like C and C++ are unable to ensure correct memory allocation and garbage collection which can thus result in buffer overflow attacks. Usage of languages that do not provide strong type checking results in such overflow and other such kinds of practical attacks. Because the C language is not strongly typed, it cannot prevent buffer overflows. Therefore, the programmer should implement safe programming techniques to make such attacks impossible in practice. Good coding practices will check for boundary limits and ensure that functions are properly called, and allocations are performed under limits. So, secure languages like JAVA should be used for thwarting such attacks(Cyber security and Communications at US Dept. of Homeland Security, 2013).

CL-2: CI-4: Buffer overflow: A buffer overflow is an anomaly where a program, while writing data to the memory, overruns the boundaries of the specific block length provided for its use and in turn overwrites adjacent memory areas. Hence, it interferes with the normal execution of the program. While buffer overflows may be a side effect of poorly written code, they can also be triggered intentionally to create an attack. This is a well-known attack and hence, needs to be taken into consideration while ensuring Cloud security. A buffer overflow can allow amalicious Cloud insider or user to load a remote shell or execute a command, enabling the attacker to gain unauthorised access or escalate user privileges in the Cloud. Once the stack is smashed, the attacker can deploy his or her payload and take control of the attacked system(Krutz R.L. and Vines R.D., 2010).

CL-2: CI-5: Input validation and content injection: When the user is logging into the Cloud interface and providing the authentication information, it should be verified and validated by the Cloud service provider. Content injection is a kind of SQL injection attack in which the Cloud user's input is applied to the SQL statements. These statements are executed by the server to launch sophisticated attacks.

CL-2: CI-6: Trojan Horses and Malware: Trojan horses hide malicious codes inside a host program that seems to do something useful. Once these programs are executed, the Virus, Worm, or other type of malicious code hidden in the Trojan horse program is released to attack the workstation, server or network. This is to allow unauthorised access to or unwanted operations on those devices. The effect of Trojans can be drastic over Cloud.

2.2.3 CL-3: Application layer security attack: The attacks identified based on threats onthe Application layer are classified as follows(Kavitha V. and Subhasini S., 2011):

CL-3: DS-1: DDoS attack: The distributed denial of service attack is from one of the application layer's security attackson the Cloud application layer. It is a specialised form of the denial of service attack that is launched by an attacker with the help of a huge number of compromised machines distributed across the internet (generally referred to as bots, the network is referred to as botnets). The purpose is to make some known and targeted web resources unusable in a Cloud environment.

CL-3: IM: Classification by invalid modification: The classification of attacks based on the invalid modifications to data or information residing in a virtual machine's host operating system are as follows:

CL-3: IM-1: Cookie poisoning: Cookie poisoning is a technique that is used by attackers for the modification of cookie information so as to make unauthorised access to Cloud interfaces and applications. Cookies are generally used to store the data related to a user's identity, such as user specific credentials etc. If the attack is launched on a Cloud and the content of the cookies of various users becomes accessible, then these can be easily forged using sophisticated techniques by an attacker. In this way, the attacker can impersonate an authorised user.

CL-3: IM-2: Backdoor and debug options: When a website is published, some of the developers enable debug options. This helps the developers to modify the code and implement changes on the website. So in other words, it can be said that this debug options provides a backdoor entry to the developers to make changes in the code. Likewise, it can also provide a backdoor to hackers and enable them to make changes at the application development level which may result in drastic effects for web resources in Cloud.

CL-3: IM-3: CAPTCHA breaking: As we know, various attacks on the Internet are launched through bots and are automated. CAPTCHAs were developed as a solution to prevent bots from using the internet resources and performing their overexploitation. However, recently it was noticed that attackers have been breaking the CAPTCHA schemes provided by the email service providers. For breaking the CAPTCHA scheme, they generally deploy and use an audio system that reads the CAPTCHA characters which are provided for the usage of visually impaired users. They use speech to text conversion for breaking it. Similarly, in one of the cases of CAPTCHA breaking, it was discovered that CAPTCHA breaking takes place because the users are provided with motivations by the automated systems, towards solving the CAPTCHAs.

CL-3: IM-4: Hidden Field Manipulation: Hidden field manipulation is a hacking practice in which the data stored in the hidden fields are manipulated. During a client's session, developers can take the help of hidden fields to store information related to the client. If this vulnerability is exploited,this may result in severe security violations by exposing the crucial information of a website.

CL-3: IM-5: Google Hacking: One of the terms that had been introduced recently is Google Hacking. It refers to the usage of the Google search engine by the hacker for obtaining useful and sensitive information while hacking a user's account. As we all know, Google today is the best and easiest way to search for details pertaining to anything on the Internet. Similarly, hackers use Google to know about the system they want to hack by gathering information, such as the security loopholes and vulnerabilities present in them. The information that is gathered will help them to carry out specific attacks on the targeted systems.

3. TAXONOMY OF DEFENCE MECHANISMS FOR CLOUD SECURITY

Figure 2 provides the Taxonomy of the Defence mechanisms for ensuring Cloud Security. The seriousness in solving Cloud security related problems with the increased frequency of attacks on the Cloud system, has led to numerous proposals for defence mechanisms. Based on our analysis of the various threats and attacks possible on Cloud, we have identified and enlisted the defence

mechanisms for their prevention. This section covers various defensive mechanisms for ensuring Cloud security to provide a roadmap of a securer Cloud environment for the future. The classification of such mechanisms is as follows:

3.1 DD: Classification by deployment of defence mechanisms

As we have seen, the attacks on Cloud security can occur at any location, be it the client side or server side. Hence, the defence mechanisms also need to be deployed at specific points so as to counter those attacks. Based on the location of the deployment, the defence mechanisms can be classified as follows:

DD-1: Cloud service user's end: Here, Cloud security defence mechanisms are deployed at the Cloud service user's end. The victim network protects him/her from attacks arising from Cloud security threats. Moreover, it responds to the detected attacks by deploying necessary counter mechanisms, such as Intrusion detection systems and Intrusion prevention systems, at the client VMs (Cloud user's end). These mechanisms help the end users to protect their confidential data from unauthorised access and ensure the integrity of the information throughout its use.

DD-2: Cloud service provider's end: The Cloud service provider protects the network using the best of technologies. Many companies which provide Cloud services are taking initiatives to provide Security as a service. This is a new buzz word in the Cloud industry. One of the world's largest technology companies, Google, has invested a lot of money into the Cloud space. It recognises that having a reputation for security is a key determinant of success. At the Cloud service provider's end, such as at Cloud hosts, Hypervisor or Cloud management units, Intrusion detection and prevention systems must be deployed to provide centralised security services.

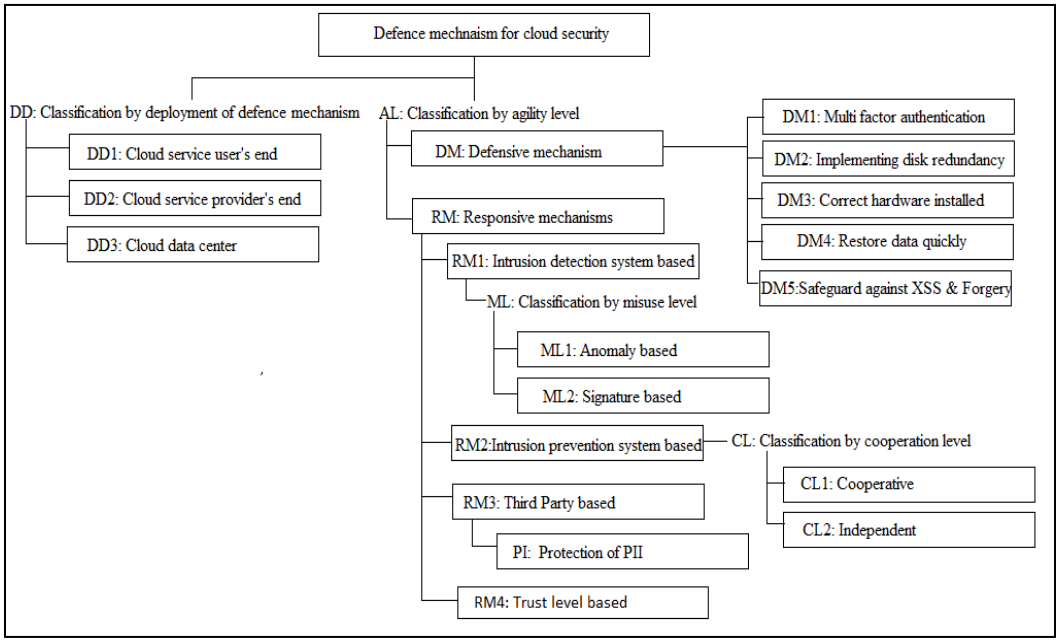

Figure2.Taxonomy of Defense Mechanisms for Cloud Security

DD-3: Cloud data centre: The decision to host your data centre somewhere else or to move some of your operations into a Cloud is never trivial. The chief concerns are security and

reliability related aspects including disaster recovery plans that meet specific requirements. The goal of using a Cloud data centre is in eliminating worries about sending critical traffic data over public lines on the Internet that lacks security. Replication can be carried outto ensure data storage security. Hence, there is a great need to look into the deployment of security and availability measures at the Cloud data centre. Therefore, security measures should be deployed and maintained for ensuring security at data centres.

3.2 AL: Classification by agility level: Based on the agility level of Cloud defence mechanisms, a classification of defensive and responsive mechanisms has beenidentified and is provided as follows:

AL: DM: Defensive mechanisms: Defensive mechanisms are techniques which a Cloud service user should check for while taking services from a Cloud service provider. Furthermore, the Cloud service provider mustensure these security services while giving services to their users. The details of such defensive mechanisms that should be looked for while buying and/or providing Cloud services include:

AL: DM-1: Multifactor authentication: The use of multi-factor authentication is where a Cloud server should authenticate every user by validating and verifying his/her login credentials along with some other user specific information. Such information could be a specific RFID or a smart card allocated to the user towards the services he/she wants to access. This multifactor authentication scheme enhances the authentication security for important resource access in the Cloud environment. Web browser and desktop access should be encrypted with Secure Socket Layer protocols. Data kept in the databases should also be kept in an encrypted form. The use of this defensive mechanism will reduce the risk of various top threats identified over Cloud that are launched through a lack of authentication and data hiding features.

AL: DM-2: Implementing disk redundancy: Implementing disk redundancy is a storage technology that enhances reliability via redundancy, and efficiency via parallel communication. This is achieved by RAID (redundant array of inexpensive disks) that combines multiple disk drives into a logical unit. In this unit, the data is distributed across the drives in one of the several ways generally referred to as RAID levels. This concept is an example of storage virtualisation. Hence, disk redundancy, if used in the Cloud infrastructure, will help to increase the data redundancy and access efficiency which is in great demand today. This will also ensure data security to its users and hence, needs to be taken into consideration while deploying a Cloud environment.

AL: DM-3: Correct hardware installed: Cloud service providers should have the correct and patched hardware installed on their systems. This would make it difficult for attackers to attack the system by exploiting well-known un-patched vulnerabilities or loopholes at the hardware level. The Cloud provider's hardware should contain high-end firewalls and routers as well as redundant independent storage units. The collocation facilities should be locked and guarded under video surveillance, and possess strong physical access controls. If this is taken care of, it will decrease a huge amount of risk on the Cloud that results from the exploitation of improper configuration and well-known vulnerabilities.

AL: DM-4: Restore data quickly: Cloud service providers should be able to restore data quickly in case hackerserase files or data from the network and local storage units. If you use a good Cloud service provider, your data will still remain safe on the Cloud (unless you have explicitly requested it to be deleted). Your provider should have the capacity to quickly restore all your data

with the click of a button. Nice control over the restoration and recovery of data is a quality factor of the Cloud environment. This will increase the quality of service even in the case of some attacks happening on the Cloud such as Distributed Denial of Service (DDoS) on data storage.

AL: DM-5: Safeguard against XSS and forgery: If a hacker gets access to the password database of Cloud users, he/she may get unauthorised access to user accounts. To prevent such scenarios, passwords must be scrambled during their storage in the database through encryption schemes. In this way, they remain secure and unusable directly by an unauthorised user, even after getting its access. File names should be obfuscated so that metadata doesn't reflect the original file data. In this way, data of a particular Cloud user or vulnerable application cannot be marked by the attacker. To make it even harder for hackers, customer data should be segregated and every request validated with tamper-proof, user-identity credentials -- even for sessions that take place offline. A service provider must take into account such mechanisms to make its service more secure and available for its Cloud users.

AL: RM: Responsive mechanisms: Responsive mechanisms are reactive techniques which a cloud service provider or a third party should provide for securing Cloud. Responsive mechanisms strive to reduce the impact of an attack on the victim. To attain this goal, theyproactively detect the attacks and respond to them so as to decrease or control the attack severity. This can be achieved with intrusion prevention systems. Responsive mechanisms are categorised as follows:

AL: RM-1: Intrusion Detection System based: Adistributed intrusion detection system (IDS) is a collection of sensors deployed at weak points in a system for monitoring the host and the network. They possess logic for detecting security breaches, logging of information and signallingalerts. The classification of intrusion detection systems that can be deployed in Cloud is as follows(Xin W., Huang T.L., and Liu X.Y., 2010).

AL: RM-1: ML: Classification by misuse level: On the basis of the technology used for detecting misuse, intrusion detection systems can be classified as anomalybased and signaturebased. Every different type of intrusion detection mechanism has its own advantages and drawbacks in terms of efficiency, performance and degree of security. These are considered in the final selection for securing Cloud deployments. Their descriptions of areas follows:

AL: RM-1: ML-1: Anomaly based: A Statisticalanomaly-based ID creates a normal profile of the Cloud in terms of either the individual Client VM's behaviour of the Cluster, or at the highest level, the Cloud system as a whole. It records the normal activities of Cloud on various parameters which are the basis for detecting an anomaly, some of them include the bandwidth utilised by an application at a Client the bandwidth utilised by an application accumulated over the Cloud as a whole, the protocols used, CPU utilisation etc. Such systems alert the administrator or user whenever something anomalous is detected which does not lie in the normal profile of the system that is gathered statistically over time. It checks for deviations from the normal behaviour for detecting anomalies.

AL: RM-1: ML-2: Signature based: A Signature-based IDS monitors and search for malicious packets in the Cloud Network, or malicious system calls or sequences in the host orat individual Client VMs. It compares them with pre-configured and pre-determined attack patterns, known as signatures present in the corresponding signature databases, to give an alert of an intrusion.

AL: RM-2: Intrusion Prevention System based: The Intrusion Prevention system (IPS), also known as the reactive system, not only performs intrusion detection in Cloud at the Client VMs or hosts but also auto-responds to the malicious activities with certain actions. These actions include shutting down malicious VMs or stopping network communications with malicious nodes launching DDoS attacks. It can also respond to network attacks by reprogramming the firewall to block the network traffic from the suspected malicious source. This means it is not only a detection system that alerts the administration of an attack but it also, by itself, takes necessary actions appropriate at that moment to thwart attacks from Cloud or comprising systems.

AL: RM-2: CL: Classification by cooperation level: This classification of Intrusion detection and prevention systems is on the basis of the extent of cooperation for intrusion detection in Cloud and as follows:

AL: RM-2: CL-1: Cooperative: The Cooperative Intrusion prevention system sends warning messages to other IPS's in other Cloud computing regions (A region is a collection of Clusters or hosts or can be a group of Client VMs with individual intrusion detection systems) about specific attacks detected by them. And then, the cooperative modules or the correlation modules are used to gather alert messages from various IPS', for identifying and deciding whether they are true or false. If they are true, the necessary actions are taken into consideration. One of the advantages of such cooperative systems is that the cooperation and communication saves the system from a single point of failure attack. It also helps in the early detection of the same kind of attacks in Cloud.

AL: RM-2: CL-2: Independent: The Independent and Individual intrusion prevention systems run on a single Client VM or host independently anddo not cooperate and/or communicate with each other. They detect attacks on their own and take security measures to respond to those attacks by their own logic. These systems, however, are unable to detect well planned distributed denial of service attacks. A secure Cloud must take into practice these defence mechanisms for thwarting network and host-based attacks on its environment.

AL: RM-3: Third party based: These are the defensive mechanisms that should be taken into practice by Cloud providers so as to reduce risks over it from third party vendors which provide services to its users.

AL: RM-3: PI: Protection of personally identifiable information: A user's personal information like SSN, credit card details, and login details should not be visible to a third party vendor providing a service either to Cloud users or to the Cloud service provider internally. An authentication mechanism provided by a third party should be such that it must not require the disclosure of the identity of a Cloud user on un-trusted hosts. Various mechanisms are available for implementing such a scheme and are given in Ranchal R., et al., (2010).

AL: RM-4: Trust level based: Users should be allowed to access the Cloud system on the basis of the trust level. For example,when a user is assigned a VM by the system for the first time and there is no information about the Cloud user and its trust profile for determining which security level of detection is suitable for the user, then a high level of security checking mechanism should be assigned to the user. That is, the user should be kept under constant and rigorous security checks so that the system can be secured from attacks from new users which may be attackers(Angin P., et al. 2010). After this, the Cloud Computing system can check theuser's behavior. After this, the Cloud Computing system can check theuser's behaviorperiodically and canthen decrease the security level or increase the trust level of a user if he/she uses the Cloud

computing services in an authorised manner without any anomalous be haviour. In this way, trust level-based access to resources will help in increasing the security in the Cloud environment from nefarious users and insiders(Kai H., Kulkareni S. and Hu Y., 2010).

4. CONCLUSIONS

Cloud Computing has revolutionised the computing world but it is prone to manifold security threats varying from network level threats to host, hypervisor and application level threats. In order to keep the Cloud secure, these security threats need to be identified and controlled and mitigated. Moreover, data residing in the cloud is prone to a number of threats. Hence, various issues like confidentiality and the integrity of data must be considered while buying storage services from a Cloud service provider. Auditing of the Cloud at regular intervals needs to be performed to safeguard the Cloud against external threats.

This paper has identified the critical threats that exist in a Cloud environment from both the Cloud users' and Cloud service providers' perspectives that should be taken care off while buying or delivering services in Cloud for ensuring high level of security towards well-known or derivable attacks. Furthermore the studyh as identified the critical risk from such attacks and the threatsthroughout the Cloud environment. This paper has also described attacks and/or threats that are possible in a Cloud computing environment based on the well-known vulnerabilities that can be exploited at various locations and layers of Cloud architecture. Also, it has also given an overview of the attacks that can be launched in the future on a Cloud environment with their criticality and impacts has been identified and listed. Defence taxonomy is also described and discussed to counter the attacks and vulnerabilities from the threats existing in Cloud environment. The Cloud security attack taxonomy and defence taxonomy outlined in this paper are useful as they clarify the security implications and needs in a secure Cloud. Further, theyprovide the directions and measures to look upon for effective solutions towards thwarting them and also for understanding and solving the problem of security attacks on a Cloud environment. In summary, the paper has analysed various vulnerabilities leading to threats andhas provided taxonomy of various attacks possible on Cloud with possible defensive solutions that can thwart such attacks in the defence taxonomy. The article will help both academia and industry to understand the challenges on security over a Cloud environment and the ways to solve them for secure Cloud services in the near future.

REFERENCES

[1] Angin P., Bhargava B., Ranchal R., Singh N., Linderman M., Othmane L.B. and Lilien L., (2010), 'An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing', Proceedings of the 29th IEEE symposium on Reliable Distributed Systems (IEEE), ISBN: 1060-9857, Oct. 31 2010-Nov. 3 2010, New Delhi, INDIA, 177-183.

[2] Brown E., (2012) 'NIST Issues Cloud Computing Guidelines for Managing Security and Privacy', National Institute of Standards and Technology Special Publication, 800-144.

[3] Buyya R. Chee Shin Yeo and Venugopal S., (2009), 'Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities' Proceedings of the 10th International Conference on High Performance Computing and Communications (IEEE), ISBN: 978-0-7695-3352-0, 25-27 September 2008 Dallan, 5-13.

[4] R. Buyya, et al., "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. 6, 2009, pp. 599-616; DOI http://dx.doi.org/10.1016/j.future.2008.12.001.

[5] Cyber security and Communications at US Dept. of Homeland Security, (2013), 'CAPEC: WASC Threat Classification 2.0', [Online], [Retrieved March 23, 2013], http://capec.mitre.org/data/definitions/333.html

[6] Chi-Chun L., Chun-Chieh H. and Joy K., (2010) 'A Cooperative Intrusion Detection System Framework for Cloud Computing Networks', Proceedings of the 39th International Conference on Parallel Processing Workshops (IEEE Computer Society), ISBN: 978-0-7695-4157-0, 13-16 September 2010, San Diego, CA 280-284.

[7] Computer Security Division, (2007), 'Recommended Security Controls for Federal Information Systems', National Institute of Standards and Technology Special Publication, 800-54 (Rev. 2).

[8] Danchev D., (December 9, 2009), 'Zeus crimeware using Amazon's EC2 as command and control server', [Online], [Retrieved October 30, 2012], http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110

[9] Dhage S.N. and Meshram B.B., (2012), 'Intrusion detection system in cloud computing environment', International Journal of Cloud Computing (Inderscience Publishers), 1 (2/3 2012), 261-282

[10] A. Goscinski and M. Brock, "Toward higher level abstractions for cloud computing," International Journal of Cloud Computing, vol. 1, no. 1, pp. 37-57; DOI 10.1504/ijcc.2011.043245.

[11] Kai H., Kulkareni S. and Hu Y., (2010), 'Cloud Security with Virtualized Defense and Reputation-Based Trust Management', Proceedings of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (IEEE), ISBN: 978-0-7695-3929-4, 12-14 December, 2009, Chengdu, 717-722.

[12] Kavitha V. and Subhasini S., (2011), 'A survey on security issues in service delivery models of cloud computing', Journal of Network and Computer Applications, 34 (1), 1-11

[13] Krutz R.L. and Vines R.D., (2010), Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley publishers.

[14] Kwon H., Kim T., Yu J.S. and Kim, K.H., (2011), 'Self-similarity Based Lightweight Intrusion Detection Method for Cloud Computing Intelligent Information and Database Systems', Lecture Notes in Computer Science, (Springer Berlin Heidelberg), 6592, 353-362

[15] Los R., Gray D., Shackleford D., and Sullivan B., (2012), 'Top Threats to Cloud Computing', [Online], [Retrieved November 23, 2012], https://cloudsecurityalliance.org/research/top-threats/

[16] Martinez C.A., Echeverri G.I. and Sanz A.G.C., (2010) 'Malware detection based on Cloud Computing integrating Intrusion Ontology representation' Proceedings of the Latin-American Conference on Communications (IEEE), ISBN: 978-1-4244-7171-3, 15-17 September, 2010, Bogota, 1-6

[17] Mazzariello C., Bifulco R. and Canonico R., (2010), 'Integrating a network IDS into an open source Cloud Computing environment', Proceedings of the 6th International Conference on Information Assurance and Security (IEEE), ISBN: 978-1-4244-7407-3, 23-25 August 2010, Atlanta, GA, 265-270

[18] McMillan R., (December 10, 2009), 'Hackers find a home in Amazon's EC2 Cloud', [Online], [Retrieved September 20, 2012], http://www.infoworld.com/d/cloud-computing/hackers-find-home-in-amazons-ec2-cloud-742

[19] Metz C., (October 5, 2009), 'Attack on Amazon Cloud Services, Bitbucket's servers down', [Online], [Retrieved October 27, 2012], http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage

[20] Perilli A. et al., (Nov 20, 2009), 'Cloud Computing Security Risk Assessment', European Union Agency for Network and Information Security, [Online], [Retrieved January 20, 2013], http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[21] Ranchal R., Bhargava B., Othmane L.B., Lilien L., Kim A., Kang M. and Linderman M., (2010) 'Protection of Identity Information in Cloud Computing without Trusted Third Party', Proceedings of the 29th IEEE symposium on Reliable Distributed Systems (IEEE), ISBN: 1060-9857, Oct. 31 2010-Nov. 3 2010, New Delhi, INDIA, 368-372

[22] Reiher P. and Mirkovic M., (2004), 'A taxonomy of DDoS attack and DDoS defense mechanisms', ACM SIGCOMM Computing Communication Review, 34 (2), 39-53

[23] S. Gupta, et al., "A Hybrid Intrusion Detection Architecture for Defense against DDoS Attacks in Cloud Environment Contemporary Computing," Communications in Computer and Information Science 306, Springer Berlin Heidelberg, 2012, pp. 498-499.

[24] S. Gupta, et al., "A fingerprinting system calls approach for intrusion detection in a cloud environment," Proc. Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on, IEEE, 2012, pp. 309-314.

[25] S. Gupta, et al., "A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment," International Journal of Distributed Sensor Networks, vol. 2013, pp. 12; DOI 10.1155/2013/364575.

[26] Vieira K., Schulter A., Westphall C.B. and Westphall C.M., (2009), 'Intrusion Detection for Grid and Cloud Computing', IT Professional, 12 (4), 38-43.

[27] Xin W., Huang T.L., and Liu X.Y., (2010), ' Research on the Intrusion detection mechanism based on cloud computing', Proceedings of the International Conference on Intelligent Computing and Integrated Systems (IEEE), ISBN: 978-1-4244-6834-8, 22-24 October, 2010, Guilin, 125-128.