Cloud Computing Environment – Security Concern

Ms, Biju Ramesh

Assistant Professor,
SIES College of Arts, Science and Commerce, Sion(W),
University of Mumbai,
India
bijuramesh_2000@yahoo.com

Abstract **- Cloud Computing enables universal, on-demand network access to a shared pool of computing resources (e.g., networks, servers, storage, applications, and services) that can be provisioned and released with minimal management effort or service provider interaction. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's existing capabilities. Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters. Because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing. Cloud Computing leverages many existing technologies such as web services, web browsers, and virtualization, which contributes to the evolution of cloud environments. Therefore, any vulnerability associated to these technologies also affects the cloud, and it can even have a significant impact. Of all the vulnerabilities data storage and virtualization are the most critical ones and an attack to them can do the most harm. This paper also describes the threats that are related to the technology used in cloud environments, and it indicates what cloud service models are exposed to these threats. The paper emphasis on threats those are associated with data being stored and processed remotely, sharing resources and the usage of virtualization. This work also discusses the countermeasures for some threats like Account or service hijacking, data leakage, customer data manipulation, VM escape, malicious VM creation, insecure VM migration and sniffing/spoofing virtual networks.**

Keywords **— Cloud Computing, security, virtualization, account hijacking, data leakage.**

I. INTRODUCTION

Cloud Computing has been envisioned as the next generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1]. Cloud Computing has emerged as a very well-known technique to support large and voluminous data with the help of shared pool of resources and large storage area. Zhiguo Wan et al. [2] states that "Cloud computing is a new computing paradigm that is built on virtualization, distributed computing, utility computing and service-oriented architecture." Further it is added that cloud computing has emerged as one of the most significant paradigm of the IT industry and has attracted most of the industry and academia. Peter Mell and Timothy Grance, [3] have defined cloud computing as "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while their software and data are stored on the servers [4]. In some respects, Cloud Computing represents the maturing of these technologies and is a marketing term to represent that maturity and the services they provide [5]. Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters [6]. Because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing [7]. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing [8]. Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form [9]. Security controls in Cloud Computing are, for the most part, no different than security controls in any IT

environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, Cloud Computing may present different risks to an organization than traditional IT solutions.
Unfortunately, integrating security into these solutions is often perceived as making them more rigid [10].

II. CHALLENGES TO CLOUD SECURITY

Security has been one of the most challenging issues for the IT executives particularly in cloud implementation. There exist numerous security anxieties that are preventing companies from captivating advantages of the cloud. Several studies, including the one by Amit Sangroya et al. [11] quote security as the primary level confront for cloud users. In this section taxonomy related to cloud computing security has been presented.

Table 1 represents the hierarchy of the cloud computing, with security challenges on both the cloud computing models: Deployment and Service models and also the issues related to Networks. The classification provided above reveals various common challenges under cloud computing. The Deployment model is classified further as Private, Public and Hybrid Cloud and the security issues of the same have been exposed in common. Further, the Service model is classified into the SaaS, PaaS and IaaS briefing its security challenges in common. The security challenges with respect to network is also shown as for any internet based service, network is considered as the backbone for cloud computing.

TABLE I
CLASSIFICATION OF SECURITY CHALLENGES

Cloud Computing Security Challenges						
Deployment Models			**Service Models**			**Network Issues**
Private	**Public**	**Hybrid**	**SaaS**	**PaaS**	**IaaS**	
Cloning and Resource Pooling			Data Leakage Problems			Browser Security
Motility of Data and Data residuals			Malicious Attacks			SQL Injection Attack
Elastic Perimeter			Backup and Storage			Flooding Attack
Shared Multi-tenant Environment			Shared Technological Issues			XML Signature Element Wrapping
Unencrypted Data			Service Hijacking			Incomplete Data Deletion
Authentication and Identity Management			Virtual Machine Hopping			Locks In

A. Deployment Models and its Security Challenges

There exist three basic types of deployment models, namely Private, Public and Hybrid clouds. Private cloud model is generally deployed within an organization and is limited only for the internal access by individuals of that organization. Public cloud model is employed by the organization for gaining access to various resources, web applications, and services over any of internet, intranet as well as extranet. Hybrid cloud is the combination of two or more clouds (public and/or private). It is an environment providing multiple service suppliers, both internal and external.
Various security challenges related to these deployment models are discussed below:

• *Cloning and Resource Pooling*: Cloning deals with replicating or duplicating the data. According to Bernd Grobauer et al. [12], cloning leads to data leakage problems revealing the machine's authenticity. While Wayne A. Pauley [13] describes resource pooling as a service provided to the users by the provider to use various resources and share the same according to their application demand. Resource Pooling relates to the unauthorized access due to sharing through the same network. While the study on Virtual and Cloud Computing by various researches states that a Virtual Machine can easily be provisioned, they can also be inversed to previous cases, paused, easily restarted, readily cloned and migrated between two physical servers, leading to non-auditable security threats.

• *Motility of Data and Data residuals:* For the best use of resources, data often is moved to cloud infrastructure. As a result the enterprise would be devoid of the location where data is put on the cloud. This is true with public cloud. With this data movement, the residuals of data is left behind which may be accessed by unauthorized users. According to Rohit Bhadauria et al. [14], data-remnant causes very less security threats in private cloud but severe security issues may evolve in public cloud donations. This again may lead to data security threats like data leakage, data remnants and inconsistent data, as stated by Hassan Takabi et al. [15]. The authors have also mentioned that in order to solve the problems with data storage the optimal solution of cryptography can be thought of effectively.

• *Elastic Perimeter:* A cloud infrastructure, particularly comprising of private cloud, creates an elastic perimeter. Various departments and users throughout the organization allow sharing of different resources to increase facility of access but unfortunately lead to data breach problem. In private clouds, according to Krishna Subramanian [16], the resources are centralized and distributed as per demand. The resource treatment transfers resources based on the requirements of the users thus leading to problems of data loss, where any user may try to access secure data with ease. Moreover, Marios D. Dikaiakos et al. [17] states that elasticity of various cloud based resources would lead to store replicated data on untrusted hosts and this would then lead to enormous risks to data privacy.

• *Shared Multi-tenant Environment:* Kui Ren et al. [18] define multitenancy as one of the very vital attribute of cloud computing, which allows multiple users to run their distinct applications concurrently on the same physical infrastructure hiding user data from each other. But the shared multi-tenant character of public cloud adds security risks such as illegal access of data by other renter using the same hardware. A multi-tenant environment might also depict some resource

contention issues when any tenant consumes some unequal amount of resources. This might be either due to genuine periodic requirements or any hack attack. Hsin-Yi Tsai et al. [19], has shown that multi-tenancy makes the impact of VM Hopping attack potentially larger than conventional IT environment.

• *Unencrypted Data:* Data encryption is a process that helps to address various external and malicious threats. Unencrypted data is vulnerable for susceptible data, as it does not provide any security mechanism. These unencrypted data can easily be accessed by unauthorized users. According to Cong Wang et al. [20], unencrypted data risks the user data leading cloud server to escape various data information to unauthorized users. For example, the famous file sharing service Dropbox was accused for using a single encryption key for all user data the company stored. These unencrypted, insecure data, as per Marjory S. Blumenthal [21], incite the malicious users to misuse the data one or the other way.

• *Authentication and Identity Management:* With the help of cloud, a user is facilitated to access its private data and make it available to various services across the network. Identity management helps in authenticating the users through their credentials. But according to Rosa Sánchez et al. [22], a key issue, concerned with Identity Management (IDM), is the disadvantage of interoperability resulting from different identity tokens and identity negotiation protocols as well as the architectural pattern. While Jianyong Clien et al. [23] have mentioned that IDM leads to a problem of intrusion by unauthorized users. They even discussed that in order to serve authentication, apart from providing a password, a multi-factor authentication using smart card and fingerprint must be implemented for attaining higher level of security.

B. Service Models and their Security Challenges

Various cloud services like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are delivered and used in real time over the cloud. Bhaskar Prasad Rimal et al. [24] have mentioned SaaS as a multi tenant platform which is commonly referred to as Application Service Provider aiding distribution of services across cloud users. While the PaaS provides the developers a platform to work with all the environments and systems for the developing, testing and deploying web applications through the cloud service. The computer infrastructure needed for this application to run on a particular platform is provided by IaaS which may give more flexibility and pay-as-you-go scheme. According to John Viegga [25], the users of SaaS have to rely heavily on the cloud provider for security purposes without any assurance to the data protection of users. In PaaS, the cloud providers offer some controls to the users building applications on their platform, without ensuring them the threats with network or intrusion prevention. While with IaaS, the developers have a better control over the application. This addresses proper security and compliance.

Various security challenges with the service models are discussed below:

• *Data Leakage and consequent problems*: Data deletion or alteration without backup leads to certain drastic data-related problems like security, integrity, locality, segregation and breaches. This would lead to sensitive data being accessed by the unauthorized users. As its measure provided by Rafael Moreno et al. [26], cloud platforms should provide new services in order to collect context information and to perform analysis and manage data privacy so as to support applications requesting the information. One solution to this data leakage problem, as provided by Danny Harnik et al. [27], is deduplication with allowing a limitation on number of user uploads per time window. The term deduplication means storing only a single copy of redundant data and providing just a link to this copy rather than storing actual copies of this data.

• *Malicious Attacks:* The threat of malicious attackers is augmented for customers of cloud services by the use of various IT services which lacks the lucidity between the procedure and process relating to service providers. Malicious users may gain access to certain confidential data and thus leading to data breaches. Farzad Sabahi [28] has shown malicious attacks by the unauthorized users on the victim's IP address and physical server. An access control mechanism tool can be thought of to control unauthorized user in accessing secured data. Peter Mell [29], has suggested Infrastructure as a Service as one of the models that exposes challenges with using virtualization as a frontier security protection to defend against malicious cloud users.

• *Backup and Storage:* The cloud vendor must ensure that regular backup of data is implemented that even ensure security with all measures. But this backup data is generally found in unencrypted form leading to misuse of the data by unauthorized parties. Thus data backups lead to various security threats. As per the study carried by Intel IT center [30], more the server virtualization increases, a very difficult problem with backup and storage is created. Data de-duplication is listed as one of the solution to reduce backup and offline storage volumes. But discussing about de-duplication, Danny Harnik et al. [27], have shown that de-duplication in cloud storage is carried out with the misuse of data backup.

• *Shared Technological issues:* IaaS vendors transport their services in a scalable way by contributing infrastructure. But this structure does not offer strong isolation properties for a multi-tenant architecture. Hence in order to address this gap, a virtualization hypervisor intercede the access between guest operating systems and the physical compute resources. As discussed by Perez R et al. [31], in spite of several advantages, these hypervisors have exhibited flaws that have permitted guest operating systems to expand inappropriate levels of control or authority on the underlying platform. This certainly led to security issues on the cloud. Lori M. Kaufman [32] has shown the implementation of IaaS by the customer to facilitate the infrastructure or hardware usage.

• *Service Hijacking:* Service hijacking is associated with gaining an illegal control on certain authorized services by various unauthorized users. It accounts for various techniques like phishing, exploitation of software and fraud. This is considered as one of the top most threats. According to Rajnish Choubey et al. [33], account hijacking has been pointed as one of the severe threats. The chances of hijacking ones account increases considerably as no native API's are used for registering various cloud services.

• *VM Hopping:* K. Owens [34] and A. Jasti et al. [35], have concluded that with VM hopping, an attacker on one VM gains rights to use another victim VM. The attacker can check the victim VM's resource procedure, alter its configurations and can even delete stored data, thus, putting it in danger the VM's confidentiality, integrity, and availability. A requirement for this attack is that the two VMs must be operating on the same host, and the attacker must recognize the victim VM's IP address. Although PaaS and IaaS users have partial authority, Thomas Ristenpart et al. [36] have shown that an attacker can get hold of or decide the IP address using benchmark customer capabilities on the basis of various tricks and combinational inputs to fetch user's IP. Thus it can be inferred that VM hopping is a rational threat in cloud computing. Additionally, multi-tenancy makes the impact of a VM hopping attack larger than in a conventional IT environment. Because quite a few VMs can run at the same time and on the same host there is a possibility of all of them becoming a victim VMs. VM hopping is thus a critical vulnerability for IaaS and PaaS infrastructures.

• *VM Mobility:* The contents of VM virtual disks are saved as files such that VMs can be copied from one host to another host over the system or via moveable storage devices with no physically pilfering a hard drive. VM mobility might offer quick use but could show the way to security problems likewise, the rapid spread of susceptible configurations that an attacker could make use of to endanger the security of a novel host. Several types of attacks might take advantage of weaknesses in VM mobility which includes man in-the-middle attacks. The severity of the attacks ranges from leaking perceptive information, to completely compromising the guest OS. Moreover, VM mobility augments the complication of security management because it offers augmented flexibility. In the IaaS model, a provider presents resources and underlying hardware as a service and a user can produce his or her possessed computing platform by importing a personalized VM representation into the infrastructure service. The huge scale of IaaS makes VM mobility's force on confidentiality and integrity in the cloud possibly outsized than in a conventional IT environment. According to B. Grobauer [12], a PaaS provider offers a variety of pre-configured computing platform and solution stacks to the service users. The users take advantage of the libraries and APIs to build up their individual applications on a permanent computing platform by importing their VM images. Although PaaS considers virtualization as a key implementation technology, it does not hold up VM mobility, therefore this service model is not having the same security challenges as a traditional IT environment. While the confidentiality, integrity and availability of PaaS, SaaS and DaaS (Database-as-a-Service) are still open to the elements, the threats rose from IaaS.

• *VM Denial of Service:* Virtualization lets numerous VMs split physical resources like CPU, network bandwidth and memory or disk. A Denial-of-Service or DoS attack in virtualization takes place when one VM occupies all the obtainable physical resources such that the hypervisor cannot hold up more VMs and accessibility is endangered. The most excellent move towards preventing a DoS attack is to bound resource allocation using correct configurations. In cloud computing, DoS attacks could still happen as discussed by Jianyong Chen [37], but having service providers place sufficient configurations to put a ceiling on the resources owed to the VMs decreases their probability. Additionally, it is advisable to have the Service Level Agreement (SLA). This legally identifies responsibilities of the service provider and the user.

C. Network Issues in Cloud

Cloud computing mainly depends upon internet and remote computers or servers in maintaining data for running various applications. The network is used to upload all the information. With the same aspect, H.B. Tabakki et al. [38] have stated security issues with network on cloud as a prime focus. It provides virtual resources, high bandwidth and software to the consumers on demand. But in reality, the network structure of this cloud faces various attacks and security issues like cloud malware injection attack, browser security issues, flooding attacks, locks-in, incomplete data deletion, data protection and XML signature element wrapping, which are explained further below.

• *Browser Security:* Every client uses browser to send the information on network. The browser uses SSL technology to encrypt user's identity and credentials. But hackers from the intermediary host may acquire these credentials by the use of sniffing packages installed on the intermediary host. Steve Kirsch [39] states that in order to overcome this, one should have a single identity but this credential must allow various levels of assurance which can be achieved by obtaining approvals digitally. Moreover, M. Jensen [40], has shown that Web Services security (WS-security) concept on browsers work with XML encrypted messages which does not need to be decrypted at intermediated hosts.

• *SQL Injection Attack:* These attacks are malicious act on the cloud computing in which a spiteful code is inserted into a model SQL code. This allows the invader to gain unauthorized access to a database and eventually to other confidential information. Further, SQL injection attacks as described by Sara Qaisar et al. [41], uses the special characters to return the data for example in SQL scripting the query usually ends up with where clause which again may be modified by adding more rows and information in it. The information entered by the hacker is misread by the website as that of the user's data and this will then allow the hacker to access the SQL server

leading the invader to easily access and modify the functioning of a website. S. Roschke et al. [42] have discussed in their paper on how the network related issues hinder the cloud computing and have also shown the SQL injection attack as the top intrusion detection.

• *Flooding Attacks:* In this attack the invader sends the request for resources on the cloud rapidly so that the cloud gets flooded with the ample requests. As per the study carried out by IBM [43], cloud has a property to expand on the basis of large amount of request. It will expand in order to fulfil the requests of invader making the resources inaccessible for the normal users.

• *XML Signature Element Wrapping:* It is found to be a very renowned web service attack. According to Jamil [44], it protects identity value and host name from illegal party but cannot protect the position in the documents. The attacker simply targets the host computer by sending the SOAP messages and putting any scrambled data which the user of the host computer cannot understand. As per the studies carried out by researchers at Ruhr University, and mentioned by the editor Lee Garber [45], the XML Signature wrapping attack changes simply the content of the signed part of a message without tampering the signature. This would not let the user to understand the twisted data, thus misguiding and misleading the user.

• *Incomplete Data Deletion:* Incomplete data deletion is treated as hazardous one in cloud computing. According to Sara Qaisar et al. [41], when data is deleted, it does not remove the replicated data placed on a dedicated backup server. The operating system of that server will not delete data unless it is specifically commanded by network service provider. Precise data deletion is majorly impossible because copies of data are saved in replica but are not available for usage.

• *Locks in:* Locks in is a small tender in the manner of tools, standard data format or procedures, services edge that could embark on data, application and service portability, not leading to facilitate the customer in transferring from one cloud provider to another or transferring the services back to home IT location.

In order to effectively utilize the cloud computing technology, the research community needs to take practical and positive measures to guarantee security. According to Gunnar Petterson [46], an association exists to assume universal standards to ensure inter-operability amongst service providers. The attempts to expand security standards to warrant data's Confidentiality, Integrity and Availability, together known as CIA, are incorporated in this effort. Moreover, Kleber Vieira et al. [47] have stated that the network must be correctly trained to efficiently detect intrusions. Hence, one should count the network related issues and try to avoid them.

III. *VULNERABILITIES AND THREATS IN CLOUD COMPUTING*

The vulnerabilities in cloud computing are the following:

i) Lack of employee screening and poor hiring practice: Some cloud providers may not perform background screening of their employees or providers[48].

ii) Lack of customer background checks: Most cloud providers do not check their customer's background, and almost anyone can open an account with a valid credit card and email [48].

iii) Lack of security education: People continue to be a weak point in information security [49]. This is true in any type of organization; however, in the cloud, it has a bigger impact because there are more people that interact with the cloud: cloud providers, third party providers, suppliers, organizational customers, and end-users.

Cloud Computing leverages many existing technologies such as web services, web browsers, and virtualization, which contributes to the evolution of cloud environments. Therefore, any vulnerability associated to these technologies also affects the cloud, and it can even have a significant impact. Of all the vulnerabilities data storage and virtualization are the most critical and an attack to them can do the most harm. There are threats that are related to the technology used in cloud environments, and it indicates what cloud service models are exposed to these threats. We put more emphasis on threats that are associated with data being stored and processed remotely, sharing resources and the usage of virtualization. Table 2 describes the various vulnerabilities in the SPI layers. Table 3 describes the threats in the SPI layers.

TABLE 2
VULNERABILITIES IN CLOUD COMPUTING

Sr. No.	Vulnerabilities	Description	Layer
V1	Insecure interfaces and APIs	Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON) [50]. The security of the cloud depends upon the security of these interfaces [48]. Some problems are: a) Weak credential b) Insufficient authorization checks c) Insufficient input-data validation Also, clouds APIs are still immature which means that are frequently updated. A fixed bug can introduce another security hole in the application [51].	SPI
V2	Unlimited allocation of resources	Inaccurate modeling of resource usage can lead to overbooking or over provisioning [52].	SPI
V3	Data-related vulnerabilities	a) Data can be colocated with the data of unknown owners (competitors, or intruders) with a weak separation b) Data may be located in different jurisdictions which have different laws [51,53] c) Incomplete data deletion – data cannot be completely removed [53] d) Data backup done by untrusted third-party providers[54] e) Information about the location of the data usually is unavailable or not disclosed to users f) Data is often stored, processed,	SPI

		and transferred in clear plain text	
V4	Vulnerabilities in Virtual Machines	a) Possible covert channels in the colocation of VMs[55] b)Unrestricted allocation and deallocation of resources with VMs [54] c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance[50,56] d) Uncontrolled snapshots – VMs can be copied in order to provide flexibility, which may lead to data leakage e) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration [56], but patches applied after the previous state disappear f) VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography [55])	I
V5	Vulnerabilities in Virtual Machine Images	a) Uncontrolled placement of VM images in public repositories b) VM images are not able to be patched since they are dormant artifacts [56]	I
V6	Vulnerabilities in Hypervisors	a) Complex hypervisor code [57] b) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited	I
V7	Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines [58]	I

TABLE 3
THREATS IN CLOUD COMPUTING

Sr. No.	Vulnerabilities	Description	Layer
T1	Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction [48].	SPI
T2	Data scavenging	Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data [52].	SPI
T3	Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed [48, 52, 55].	SPI
T4	Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.	SPI
T5	Customer-data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.	S
T6	VM escape	It is designed to exploit the hypervisor in order to take control of the underlying infrastructure.	I
T7	VM hopping	It happens when a VM is able to gain access to another VM (i.e. by exploiting some hypervisor vulnerability) [52]	I
T8	Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository.	I
T9	Insecure VM migration	Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions: a) Access data illegally during migration [50] b) Transfer a VM to an untrusted host [56] c) Create and migrate several VM causing disruptions or DoS	I
T10	Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [58].	I

IV. *COUNTERMEASURES*

Here we will discuss the countermeasures for the threats mentioned in Table 3.

i) Countermeasures for the threat account or service Hijacking:

- Identity and access management guidance:

Cloud Security Alliance (CSA) is a non-profit organization that promotes the use of best practices in order to provide security in cloud environments. CSA has issued an Identity and Access Management Guidance [59] which provides a list of recommended best practiced to assure identities and secure access management. This report includes centralized directory, access management, identity management, role-based access control, user access certifications, privileged user and access management, separation of duties, and identity and access reporting.

- Dynamic credentials [60]:

This presents an algorithm to create dynamic credentials for mobile cloud computing systems. The dynamic credential changes its value once a user changes its location or when he has exchanged a certain number of data packets.

ii) Countermeasures for the threat data leakage

- Fragmentation-redundancy-scattering(FRS) technique [61]:

This technique aims to provide intrusion tolerance and, in consequence, secure storage. This technique consists in first breaking down sensitive data into insignificant fragments, so any fragment does not have any significant information by itself. Then, fragments are scattered in a redundant fashion across different sites of the distributed system.

- Digital signatures [62]:

This proposes to secure data using digital signature with RSA algorithm while data is being transferred over the Internet.

They claimed that RSA is the most recognizable algorithm, and it can be used to protect data in cloud environments.

- Homomorphic encryption :

The three basic operations for cloud data are transfer, store, and process. Encryption techniques can be used to secure data while it is being transferred in and out of the cloud or stored in the provider's premises. Cloud providers have to decrypt cipher data in order to process it, which raises privacy concerns. In [63], they propose a method based on the application of fully homomorphic encryption to the security of clouds. Fully homomorphic encryption allows performing arbitrary computation on ciphertexts without being decrypted. Current homomorphic encryption schemes support limited number of homomorphic operations such as addition and multiplication. The authors in [64] provided some real-world cloud applications where some basic homomorphic operations are needed. However, it requires a huge processing power which may impact on user response time and power consumption.

- Encryption :

Encryption techniques have been used for long time to secure sensitive data. Sending or storing encrypted data in the cloud will ensure that data is secure. However, it is true assuming that the encryption algorithms are strong. There are some well-known encryption schemes such as AES (Advanced Encryption Standard). Also, SSL technology can be used to protect data while it is in transit. Moreover, [65] describes that encryption can be used to stop side channel attacks on cloud storage de-duplication, but it may lead to offline dictionary attacks reviling personal keys.

iii) Countermeasures for the threat customer data manipulation

- Web application scanners :

Web applications can be an easy target because they are exposed to the public including potential attackers. Web application scanners [66] is a program which scans web applications through the web front-end in order to identify security vulnerabilities. There are also other web application security tools such as web application firewall. Web application firewall routes all web traffic through the web application firewall which inspects specific threats.

iv) Countermeasures for the threat VM escape

- HyperSafe [67]:

It is an approach that provides hypervisor control-flow integrity. HyperSafe's goal is to protect type I hypervisors using two techniques: nonbypassable memory lockdown which protects write protected memory pages from being modified, and restricted pointed indexing that converts control data into pointer indexes. In order to evaluate the effectiveness of this approach, they have conducted four types of attacks such as modify the hypervisor code, execute the injected code, modify the page table, and tamper from a return table. They concluded that HyperSafe successfully prevented all these attacks, and that the performance overhead is low.

- Trusted cloud computing platform :

TCCP[68] enables providers to offer closed box execution environments, and allows users to determine if the environment is secure before launching their VMs. The TCCP adds two fundamental elements: a trusted virtual machine monitor (TVMM) and a trusted coordinator (TC). The TC manages a set of trusted nodes that run TVMMs, and it is maintained but a trusted third party. The TC participates in the process of launching or migrating a VM, which verifies that a VM is running in a trusted platform. The authors in [69] claimed that TCCP has a significant downside due to the fact that all the transactions have to verify with the TC which creates an overload. They proposed to use Direct Anonymous Attestation (DAA) and Privacy CA scheme to tackle this issue.

- Trusted virtual datacenter :

TVDc [70,71] insures isolation and integrity in cloud environments. It groups virtual machines that have common objectives into workloads named Trusted Virtual Domains (TVDs). TVDc provides isolation between workloads by enforcing mandatory access control, hypervisor-based isolation, and protected communication channels such as VLANs. TVDc provides integrity by employing load-time attestation mechanism to verify the integrity of the system.

v) Countermeasures for the threat malicious virtual machine creation

- Mirage

In [72], the authors propose a virtual machine image management system in a cloud computing environments.This approach includes the following security features: access control framework, image filters, a provenance tracking, and repository maintenance services. However, one limitation of this approach is that filters may not be able to scan all malware or remove all the sensitive data from the images. Also, running these filters may raise privacy concerns because they have access to the content of the images which can contain customer's confidential data.

vi) Countermeasures for the threat insecure virtual machine migration

- Protection aegis for live migration of VMs (PALM):

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

- VNSS:

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

vii) Countermeasures for the threat sniffing/spoofing virtual networks

- Virtual network security:

Wu and et al. [58] presents a virtual network framework that secures the communication among virtual machines. This framework is based on Xen which offers two configuration modes for virtual networks: "bridged" and "routed". The virtual network model is composed of three layers: routing layers, firewall, and shared networks, which can prevent VMs from sniffing and spoofing.

V. CONCLUSIONS

Cloud computing has made end users both thrilled and edgy. They are excited by various opportunities provided by the cloud and are anxious as well on the questions related to the security it offers. As users migrate their data on cloud they would be alarmed with the security flaws inherent to the cloud environment. Thus security threats with cloud computing has emerged as one of the very plausible topics. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines. New security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies.

VI. REFERENCES

1. P. Mell and T. Grance, *"Draft nist working definition of cloud computing"*http: // csrc.nist.gov/groups/SNS / cloudcomputing /index.html.
2. Zhiguo Wan, Jun'e Liu, and Robert H. Deng, " HASBE: A Hierarchical Attribute Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, april 2012, pp: 743 – 754.
3. Peter Mell and Timothy Grance, The NIST Definition of Cloud Computing, U.S. National Institute of Standards and Technology (NIST), Special Publication 800-145, September 2011
4. Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Springer-Verlag Berlin, Heidelberg
5. Centre for the Protection of National Infrastructure (2010) Information Security Briefing 01/2010 Cloud Computing. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf
6. KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey. Available: http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs-2010-cloud-computing-survey/2384291
7. Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487
8. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA
9. Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp 69–79
10. Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
11. Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma, "Towards Analyzing Data Security Risks in Cloud Computing Environments", Springer-Verlag Berlin Heidelberg 2010, pp. 255-265.
12. Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker, "Understanding Cloud Computing Vulnerabilities", IEEE, 1540-7993/11, 2011, pp: 50-57.
13. Wayne A. Pauley, "Cloud Provider Transparency – An empirical evaluation", the IEEE computer and reliability societies, IEEE, November 2010, pp: 32 – 39.
14. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing and Associated Mitigation", International Journal of Computer Applications (IJCA), June 2012, pp: 47 – 66.
15. Hassan Takabi and James B.D. Joshi, University of Pittsburgh, Gail – Joon and Ahn Arizona State University, "Security and Privacy Challenges in Cloud Computing Environments", IEEE security and privacy, www.computer.org/security, 2010, pp. 24 – 31.
16. Krishnan Subramanian, "Private, Public and Hybrid Clouds", whitepaper: Trend Micro, 2011.
17. Marios D. Dikaiakos, George Pallis, Dimitrios Katsaros, Pankaj Mehra, Athena Vakali, "Cloud Computing – Distributed Internet Computing for IT and Scientific Research", IEEE Internet Computing, 2009 IEEE, pp: 10 – 13.
18. Kui Ren, Cong Wang, and Qian Wang, llinois Institute of Technology, "Security Challenges for the Public Cloud", IEEE Press, 2012, pp. 69 – 73.
19. Hsin-Yi Tsai, Melanie Siebenhaar and André Miede, Yu-Lun Huang, Ralf Steinmetz, "Threat as a Service? Virtualization's impact on Cloud Security", IEEE, IT Pro, 2012, pp: 32- 37.
20. Cong Wang, Ning Cao, Kui Ren, Wenjing Lou, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE transactions on parallel and distributed systems, IEEE, Digital Object Indentifier 10.1109/TPDS.2011.282, 2011, pp: 1 – 14.
21. Marjory S. Blumenthal, "Hide and Seek in the Cloud", IEEE, March – April 2010, pp: 57-58.
22. Rosa Sánchez, Florina Almenares, Patricia Arias, Daniel Díaz-Sánchez and Andrés Marín, "Enhancing Privacy and Dynamic Federationn IdM for Consumer Cloud Computing", IEEE Transactions on Consumer Electronics, Vol. 58, No. 1, February 2012, pp: 95 – 103.
23. Jianyong Chen, Yang Wang, Xiaomin Wang, "On demand Security Architecture for Cloud Computing", IEEE, 0018-9162, Digital Object Indentifier 10.1109/MC.2012.120, pp: 1 -12.
24. Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, "A Taxonomy and Survey of Cloud Computing Systems", 978-0-7695-3769-6/09, IEEE, pp: 44 – 51.
25. John Viega, "Cloud Computing and the Common Man", IEEE, 0018-9162/09, pp: 106 – 108.

26. Rafael Moreno-Vozmediano, Rubén S. Montero, and Ignacio M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services", IEEE, Digital Object Indentifier 10.1109/MIC.2012.69.
27. Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg, "Side Channels in Cloud Services: Deduplication in Cloud Storage", 540-7993/10, IEEE, 2010, pp: 40 – 47.
28. Farzad Sabahi, "Cloud Computing Security Threats and Responses", 978-1-61284-486-2, IEEE, 2011, pp: 245 – 249.
29. Peter Mell, "What's Special about Cloud Security?" , IEEE, IT Pro July/August 2012, pp: 6 – 8.
30. Intel IT Center, "Preparing your Virtualized Data Center for the Cloud", pp: 1 – 20.
31. Perez R, van Doorn L, Sailer R. "Virtualization and hardware-based security". IEEE Security and Privacy 2008;6(5):24–31.
32. Lori M. Kaufman, Bruce Potter, "Monitoring Cloud Computing by Layer, Part 1", 1540-7993/11, IEEE, pp: 66 – 68.
33. Rajnish Choubey, Rajshree Dubey, Joy Bhattacharjee, "A Survey on Cloud Computing Security, Challenges and Threats", International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol. 3 No. 3 March 2011, pp: 1227 – 1231.
34. K. Owens, "Securing Virtual Computer Infrastructure in the Cloud," white paper, Savvis Communications Corp., 2009.
35. A. Jasti et al., "Security in Multi-Tenancy Cloud," Proc. IEEE Int'l Carnahan Conf. Security Technology (ICCST 10), IEEE Press, 2010, pp. 35–41.
36. Thomas Ristenpart et al., "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security (CCS09), ACM Press, 2009, pp. 199–212.
37. Jianyong Chen, Yang Wang, Xiaomin Wang, "On demand security architecture for Cloud Computing, IEEE 2011, pp: 1 – 12.
38. H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing (CloudApp 2010), IEEE CS Press, 2010, pp. 393–398.
39. Steve Kirsch et al., "The Future of Authentication", 1540-7993/12, IEEE, January-February 2012, pp: 22 – 27.
40. M. Jensen, "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, pp: 109 – 116.
41. Sara Qaisar, Kausar Fiaz Khawaja, "Cloud Computing: Network/Security Threats and counter measures", Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com, January 2012, Vol 3, N0 9, pp: 1323 – 1329.
42. S. Roschke, et al., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2009.
43. Web 2.0/SaaS Security, Tokyo Research Laboratory, IBM Research. http://www.trl.ibm.com/projects/web20sec/web20sec_e.html
44. Jamil, D., Zaki, H. "Security issues in cloud computing and counter measures", International Journal of Engineering Science and Technology (IJEST) , Vol. 3 No. 4, pp: 2672-2676.
45. Lee Garber, "Serious Security Flaws identified in Cloud Systems", News Briefs, IEEE, December, 2011, pp: 21 – 23.
46. Gunnar Petterson, "Don't Trust and Verify: A Security Architecture Stack for the Cloud", IEEE, 1540-7993/10, pp: 83 – 86.
47. Kleber Vieira, Alexandre Schulter, Carlos Becker Westphall, and Carla Merkle Westphall, "Intrusion Detection for Grid and Cloud Computing", Published by the IEEE computer society, IEEE, July-August 2011, pp:38-43.
48. Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. Available: https://cloudsecurityalliance.org/research/top-threats
49. Popovic K, Hocenski Z (2010) Cloud Computing Security issues and challenges. In: Proceedings of the 33rd International convention MIPRO. IEEE Computer Society Washington DC, USA, pp 344–349
50. Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: Challenges and solutions. In: the 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany. IEEE Computer Society, Washington, DC, USA, pp 1–8
51. Carlin S, Curran K (2011) Cloud Computing Security. International Journal of Ambient Computing and Intelligence 3(1):38–46
52. ENISA (2009) Cloud Computing: benefits, risks and recommendations for information Security. Available: http://www.enisa.europa.eu/activities/riskmanagement/files/deliverables/cloud-computing-risk-assessment
53. Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36–42
54. Winkler V (2011) Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier Inc, Waltham, MA
55. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA. ACM New York, NY, USA, pp 199–212
56. Garfinkel T, Rosenblum M (2005) When virtual is harder than real: Security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. USENIX Association Berkeley, CA, USA, pp 227–229
57. Wang Z, Jiang X (2010) HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity. In: Proceedings of the IEEE symposium on Security and privacy. IEEE Computer Society, Washington, DC, USA, pp 380–395
58. Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing. In: 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18–21
59. Cloud Security Alliance (2012) SecaaS implementation guidance, category 1: identity and Access managament. Available: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf
60. Xiao S, Gong W (2010) Mobility Can help: protect user identity with dynamiccredential. In: Eleventh International conference on Mobile data Management (MDM). IEEE Computer Society, Washington, DC, USA, pp 378–380
61. Wylie J, Bakkaloglu M, Pandurangan V, Bigrigg M, Oguz S, Tew K, Williams C,Ganger G, Khosla P (2001) Selecting the right data distribution scheme for a survivable Storage system. CMU-CS-01-120, Pittsburgh, PA
62. Somani U, Lakhani K, Mundra M (2010) Implementing digital signature with RSA encryption algorithm to enhance the data

Security of Cloud in Cloud Computing. In: 1st International conference on parallel distributed and grid Computing (PDGC). IEEE Computer Society Washington, DC, USA, pp 211–216
63. Tebaa M, El Hajji S, El Ghazi A (2012) Homomorphic encryption method applied to Cloud Computing. In: National Days of Network Security and Systems (JNS2). IEEE Computer Society, Washington, DC, USA, pp 86–89
64. Naehrig M, Lauter K, Vaikuntanathan V (2011) Can homomorphic encryption be practical? In: Proceedings of the 3rd ACM workshop on Cloud Computing Security workshop. ACM New York, NY, USA, pp 113–124
65. Harnik D, Pinkas B, Shulman-Peleg A (2010) Side channels in Cloud services: deduplication in Cloud Storage. IEEE Security Privacy 8(6):40–47
66. Fong E, Okun V (2007) Web application scanners: definitions and functions. In: Proceedings of the 40th annual Hawaii International conference on system sciences. IEEE Computer Society, Washington, DC, USA
67. Wang Z, Jiang X (2010) HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity. In: Proceedings of the IEEE symposium on Security and privacy. IEEE Computer Society, Washington, DC, USA, pp 380–395
68. Santos N, Gummadi KP, Rodrigues R (2009) Towards Trusted Cloud Computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California. USENIX Association Berkeley, CA, USA
69. Han-zhang W, Liu-sheng H (2010) An improved trusted cloud computing platform model based on DAA and privacy CA scheme. In: International Conference on Computer Application and System Modeling (ICCASM), vol.13, V13–39. IEEE Computer, Society, Washington, DC, USA, pp V13–33
70. Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D (2008) TVDc: managing Security in the trusted virtual datacenter. SIGOPS Oper. Syst. Rev. 42(1):40–47
71. Berger S, Cáceres R, Goldman K, Pendarakis D, Perez R, Rao JR, Rom E, Sailer R, Schildhauer W, Srinivasan D, Tal S, Valdez E (2009) Security for the Cloud infrastructure: trusted virtual data center implementation. IBM J Res Dev 53 (4):560–571
72. Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of virtual machine images in a Cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud Computing Security. ACM New York, NY, USA, pp 91–96
73. Zhang F, Huang Y, Wang H, Chen H, Zang B (2008) PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In: Trusted Infrastructure Technologies Conference, 2008. APTC'08, Third Asia-Pacific. IEEE Computer Society, Washington, DC, USA, pp 9–18
74. Xiaopeng G, Sumei W, Xianqin C (2010) VNSS: a Network Security sandbox for virtual Computing environment. In: IEEE youth conference on information Computing and telecommunications (YC-ICT). IEEE Computer Society, Washington DC, USA, pp 395–398