ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

Security Issues and Countermeasures in Cloud Computing Environment

Varun Krishna Veeramachaneni
Department of Computer Science, NewYork Institute of Technology, Old Westbury, NY

Abstract- "Cloud computing" represents a relatively new computing model in the evolution of on-demand information technology services and products, that is built on decades of research in virtualization, distributed computing, utility computing, and more recently networking, web and software services. It implies a service oriented architecture, reduced information technology overhead for the end-user, great flexibility, and reduced total cost of ownership. Contrarily to traditional onsite application architecture where applications are residing in client machines or in a server accessible via client cloud computing offers shared computer application resources and accessible via the Internet. Since cloud computing share distributed resources via the network in the open environment, it presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Various categories of such security concerns are trust, architecture, identity management, software isolation, data protection, confidentiality and availability. All these security vulnerabilities lead to various threats on the cloud such as authentication, misuse of cloud infrastructure, eavesdropping, network intrusion, denial of service attack, session hijacking. Further Cloud Forensic is an emerging challenge related to cloud security]. It examines the key security issues of Cloud computing being faced today and the challenges and opportunities that it brings for business community. This research paper illustrates a brief description of what exactly cloud computing security-related issues are, and discusses data security and privacy protection issues associated with cloud computing across all stages of data life cycle. It also shows current solutions for data security and privacy protection issues in cloud. and describes future research work.

Keywords- **Cloud Computing, virtualization, distributed computing, data security, trust**

I. INTRODUCTION

The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. It has been envisioned as the next generation paradigm in computation. The economical, scalable, expedient, ubiquitous, and on-demand access to shared resources are some of the characteristics of the cloud that have resulted in shifting the business processes to the cloud. A study by Gartner [1] considered Cloud Computing as the first among the top 10 most important technologies and with a better prospect in successive years by companies and organizations. Cloud computing embraces cyber infrastructure, and builds upon decades of research in virtualization, distributed computing, "grid computing", utility computing, and, more recently, networking, web and software services. Cloud Computing appears as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [2,3]. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [4-7].

Regarding definition of cloud computing model, the most widely used one is made by NIST as "Cloud computing is a model for enabling 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.". The cloud computing model NIST defined has three service models and four deployment models. The three service models, also called SPI model, are: Cloud Software as Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). The four deployment models are: Private cloud, Community cloud, Public cloud and Hybrid cloud. Compared with the traditional IT model, the cloud computing has many potential advantages. But from the consumers' perspective, cloud computing security concerns remain a major barrier for the adoption of cloud computing.

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,

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

privacy and legal matters [8]. 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 [9]. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing [10]. Data sets consisting of so much, possibly sensitive data, and the tools to extract and make use of this information give rise to many possibilities for unauthorized access and use. Much of our preservation of privacy in society relies on current inefficiencies. Cloud facilities become a cost-effective platform for malicious agents, e.g., to launch a botnet or to apply massive parallelism to break a cryptosystem. Along with developing this technology to enable useful capabilities, we must create safeguards to prevent abuse [11]

A. Cloud computing service models

- Software as a Service (SaaS) The facility given to the user is to use the vendor's applications which are running on a cloud infrastructure. The user doesn't need to control these applications which are provided by vendor on the cloud infrastructure. In this service, services provided by the service provider are available to user
- Platform as a Service (PaaS) In this service development or software environment is provided as service upon which higher levels of services can be built means in which applications can be developed and deployed. This service provides automatic arrangement for ready to use services
- Infrastructure as a Service (IaaS) This service provides infrastructure to user with the use of storage, memory. User does not manage cloud infrastructure. But user can manage his data stored on cloud infrastructure and applications which he has deployed. Gmail, Drop box are some applications of cloud computing services.

B. Cloud Computing Deployment models

- There are three fundamental deployment models for cloud computing environment but NIST (National Institute of Standards and Technology) proposed four set of deployment models.
- Public Cloud – In this particular style of cloud infrastructure represents a cloud environment which can be publicly accessible and manageable by a corporation or an alternative cloud service provider.
- Private Cloud – This style of infrastructure is managed and operated only by private organization. The primary goal of the style of cloud model should be to sustain consistent higher level of security and privacy.
- Community Cloud – This model shares infrastructure between organizations or communities have common mission and vision such as: security, jurisdiction. Services are managed by organizations or others.
- Hybrid Cloud – This type of deployment model is composition of two or more cloud models; these are bound together but every one of them remains unique entities

II. SECURITY ISSUES OF 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. Rapid cloud adoption has however, introduced unique and complex security considerations for users. Now organizations must consider how adopting a cloud-computing model will affect their risk profile related to data security, privacy and availability. Complicating that assessment is the fact that now within the ultimate security of cloud implementations is an inherent partnership with the cloud service provider. Aspects such as physical security, configuration integrity and personnel vetting is now in the hands of the provider, which most organizations taking advantage of the cloud never see. [12]From various research articles we can conclude that data storage and virtualization are the most critical and an attack to them can do the most harm. Attacks to lower layers have more impact to the other layers. We put more emphasis on threats that are associated with data being stored and processed remotely, sharing resources and the usage of virtualization. For each vulnerability and threat, we identify what cloud service model or models are affected by these security problems. This analysis offers a brief description of the vulnerabilities, and indicates what cloud service models (SPI) can be affected by them. For this analysis, we focus mainly on technology-based vulnerabilities. Some of these vulnerabilities are the following:

A. Challenges in Cloud Communication Security

The communication process results in transmission of either data/information or applications between the customer and the cloud. Moreover, there exists communication within cloud between VMs. This communication generates cloud specific challenges because of cloud specific characteristics and technologies.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

- ***Shared communication infrastructure:***

Resource pooling not only results in sharing of computational and storage resources but also sanctions the sharing of network infrastructure components [13] The sharing of network components provides attacker the window of cross-tenant attack [14]. The vulnerability stems from the resource pooling characteristic of the cloud computing and affects the IaaS service model of the cloud. Due to the fact that it is hard to distinguish between a legal vulnerability scan of network and attacker activity, usually such scans are not allowed by the service providers. Similarly, the IP-based segregation of network portions are not applied as network resources are dynamically provisioned and released and cannot be associated to particular set of users. The users on the cloud are usually granted with the super-user access for the purpose of managing their VMs. The access capability empowers the malicious user to acquire system IP or MAC addresses and make malicious use of IaaS network interfaces. The malicious user with super-user access to the real network components may launch attacks, such as, sniffing and spoofing over the real network.

- ***Virtual network:***

In cloud computing systems, the communication takes place not only on real networks but virtualized networks also play an important role in communication. Virtual network is a logical network built over a physical network. The virtual networks are responsible for communication between VMs. The software-based network components, such as bridges, routers, and software-based network configurations, support the networking of VMs over the same host. The virtualized networks are able to generate the following security challenges in the cloud environment. Security and protection mechanisms over the physical network are not able to monitor the traffic over virtualized network. This becomes a serious challenge as malicious activities of the VMs go beyond the monitoring of security tools. Intrusion detection and prevention mechanisms usually depend on the traffic patterns and activities to judge the anomalies and detect the possibility of the attack. Virtualized network poses a hindrance to the goal of such preventive measures [15]. The virtualized network is shared among multiple VMs that causes the possibility of certain attacks, such as, Denial of Service (DoS), spoofing and sniffing of virtual network. The traffic rates can be monitored for malicious purposes. The cryptographic keys become vulnerable to leakage, in case of malicious sniffing and spoofing of virtual network [16]. The data in transit belonging to users can suffer from costly breaches

- ***Security Misconfiguration:***

Security configurations of the cloud network infrastructure are of significant importance in providing secure cloud services to the user [17]. Misconfigurations can radically compromise the security of customers, applications, and the whole system. Customers outsource their applications and data to the cloud with the trust that their assets are secure within the cloud environment. A small misconfiguration can breach the security of the system. The configurations need to be well in place not only at the time of cloud infrastructure development, deployment, and operations but subsequent changes in the cloud network should also keep the configuration consistent with the security policies. One of the most common misconfiguration occur when administrators select such a configuration tool that they are familiar with but not necessarily covers all the security requirements. The migration of VMs, data, and applications across multiple physical nodes, changes in traffic patterns, and topology can generate the requirement of varied security policies . In such a scenario, the configuration of the cloud should dynamically be managed to ensure the security of the cloud. Likewise, any weakness in session configurations and protocol configurations can be exploited for session hijacking and to gain user sensitive data.

B. Security in the SPI model

With SaaS, the burden of security lies with the cloud provider. In part, this is because of the degree of abstraction, the SaaS model is based on a high degree of integrated functionality with minimal customer control or extensibility. By contrast, the PaaS model offers greater extensibility and greater customer control. Largely because of the relatively lower degree of abstraction, IaaS offers greater tenant or customer control over security than do PaaS or SaaS. Before analyzing security challenges in Cloud Computing, we need to understand the relationships and dependencies between these cloud service models. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of these deep dependencies, any attack to any cloud service layer can compromise the upper layers. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. These relationships and dependencies between cloud models may also be a source of security risks. A SaaS

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

provider may rent a development environment from a PaaS provider, which might also rent an infrastructure from an IaaS provider. Each provider is responsible for securing his own services, which may result in an inconsistent combination of security models. It also creates confusion over which service provider is responsible once an attack happens.

- ***Software-as-a-service (SaaS) security issues:***

SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM SaaS users have less control over security among the three fundament delivery models in the cloud. The adoption of SaaS applications may raise some security concerns.

- ***Platform-as-a-service (PaaS) Security Issues:***

PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers . As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform. [PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications.

- ***Infrastructure-as-a-service (IaaS) Security Issues:***

IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet. Users are entitled to run any software with full control and management on the resources allocated to them [18]. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor [19]. They control the software running in their virtual machines, and they are responsible to configure security policies correctly [20]. However, the underlying compute, network, and storage infrastructure is controlled by cloud providers. IaaS providers must undertake a substantial effort to secure their systems in order to minimize these threats that result from creation, communication, monitoring, modification, and mobility [21]. Here are some of the security issues associated to IaaS.

C. Virtualization

Virtualization allows users to create copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications [22]. However, it also introduces new opportunities for attackers because of the extra layer that must be secured [31]. Virtual machine security becomes as important as physical machine security, and any flaw in either one may affect the other [23]. Virtualized environments are vulnerable to all types of attacks for normal infrastructures; however, security is a greater challenge as virtualization adds more points of entry and more interconnection complexity [24]. Unlike physical servers, VMs have two boundaries: physical and virtual.

- ***Virtualization issues:*** Virtualization is one of the strategic components of the cloud. Virtualization allows the use of same physical resources by multiple customers. A separate VM is instantiated for each user that virtually provides a complete operating machine to the user [25]. Several VMs can be mapped to the same physical resources allowing the resource pooling in multi-tenant environment. A VM monitor (VMM) or hypervisor is the module that manages the VMs and permits various operating systems to run simultaneously on the same physical system. Nevertheless, virtualization also introduces security challenges to the cloud users and infrastructure [26]. We discuss the security issues related to virtualization below.
- ***VM image sharing****:* A VM image is used to instantiate VMs. A user can create his/her own VM image or can use an image from the shared image repository. The users are allowed to upload and download images from the repository (for example Amazons image repository) Sharing of VM images in the image repositories is a common practice and can evolve as a serious threat if it is used in malicious manner . A malicious user can investigate the code of the image to look for probable attack point. On the other hand, a malicious user can upload an image that contains a malware. The VM instantiated through the infected VM image will become source of introducing malware in the cloud computing system. Moreover, an infected VM can be used to monitor the activities and data of other users resulting in privacy breach. Likewise, if the image is not properly cleaned, it can expose some confidential information of the user/
- ***VM Isolation****:* VMs running on the same physical hardware need to be isolated from each other. Although logical isolation is present between different VMS, the access to same physical resources can lead to data breach

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

and cross-VM attacks. Isolation is not only needed on storage devices but memory and computational hardware also needs fine grained isolation of VMs.

- ***VM escape****:* VM escape is a situation in which a malicious user or VM escapes from the control of VMM or hypervisor. A VMM is a software component that manages all the VMs and their access to the hardware. The VM escape situation can provide attacker access to other VMs or can bring the VMM down . A successful VM escape attack can provide access to the computing and storage hardware. The IaaS service model is affected that can in turn effect other service models [27].
- ***VM migration:*** The VM migration is the process of relocating a VM to another physical machine without shutting down the VM. The VM migration is carried out for a number of reasons, such as load balancing, fault tolerance, and maintenance. During the migration phase, the contents of the VM are exposed to the network that might lead to data privacy and integrity concerns. Besides data, the code of VM also becomes vulnerable to attackers during migration . The migration module can be compromised by an attacker to relocate the VM to a compromised server or under the control of compromised VMM. The VM migration is a crucial phase and needs to be carried out in a secured manner
- ***VM rollback****:* Virtualization allows the rollback of a VM to some previous state whenever it is needed. The rollback feature provides flexibility to the user. However, rollback also raises security concerns. [28] For example, the rollback can enable the security credentials that were previously disabled . Moreover, the rollback can also render the VM to a vulnerability that was previously patched. Furthermore, the rollback can revert the VM to previous security policies and configuration errors].
- ***Hypervisor issues****:* The key module of virtualization is hypervisor or VMM. The VMs management and isolation is the responsibility of the VMM. Generating and managing virtual resources, is yet another function performed by the VMM. A VMM may affect the execution of VMs running on the host system [29]. A compromised VMM can put all the VMs that are managed by the victim VMM under attacker's control [30]. The metadata of the VMs, kept by the VMM, may also be exposed to an attacker if the attacker takes control of a VMM . A VMM can provide larger attack vector due to more entry points and interconnection complexities There are many reported bugs in the VMM that let the attacker to take control of the VMM or bypass security restrictions. For example, vulnerabilities in the Xen, Microsoft Virtual PC, and Microsoft Virtual Server can be abused by attackers to gain privileged rights.
- ***VM sprawl:*** VM sprawl is a situation where a number of VMs on the host system is continuously increasing and most of the already instantiated VMs are in idle state. The VM sprawl causes the resources of the host machine to be wasted on large scale.

D. Data security

Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. Data security is a common concern for any technology, but it becomes a major challenge when cloud computing service model users have to rely on their providers for proper security. In cloud computing organizational data is often processed in plaintext and stored in the cloud. The cloud provider is the one responsible for the security of the data while is being processed and stored. Also, data backup is a critical aspect in order to facilitate recovery in case of disaster, but it introduces security concerns as well. Also cloud providers can subcontract other services such as backup from third-party service providers, which may raise concerns. Moreover, most compliance standards do not envision compliance with regulations in a world of Cloud Computing. In the world of cloud computing, the process of compliance is complex because data is located in the provider's datacenters, which may introduce regulatory compliance issues such as data privacy and integrity, data recovery vulnerability, and data backup security must be enforced by the provider.

- ***Data privacy and integrity****:* The data in the cloud is much more vulnerable to risks in terms of confidentiality, integrity, and availability in comparison to the conventional computing model. The ever increasing number of users and applications leads to enhanced security risks. In a shared environment, the security strength of the cloud equals the security strength of its weakest entity. Not only the malicious entity collocated with the victim data, but also any non-malicious but unsecure entity can result in breach of data. A successful attack on a single entity will result in unauthorized access to the data of all the users. Violation of integrity may also result from multi-tenant nature of the cloud. Data integrity is one of the most critical elements

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

in any information system. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen. Besides the data at rest, the data being processed also comes across security risks. Due to virtualization physical resources are shared among multiple tenants. This eventually may allow malicious users (sharing computing resources) to launch attacks on the data of other users while in processing phase. Moreover, if the data backup process is outsourced to a third party by the CSP, risks boundary is also broadened. The cryptographic key generation and management for cloud computing paradigm is also not standardized. Absence of secure and standard key management techniques for the cloud does not allow the standard cryptographic mechanisms to scale well to the cloud computing model. Therefore, domain of cryptography also enhances the potential risks to the data.

- ***Data recovery vulnerability****:* Due to resource pooling and elasticity characteristics, the cloud ensures dynamic and on demand resource provisioning to the users. The resource allocated to a particular user may be assigned to the other user at some later point of time. In case of memory and storage resources, a malicious user can employ data recovery techniques to obtain the data of previous users . The authors in were able to recover Amazon machine images files 98 % of the times. The data recovery vulnerability can pose major threats to the sensitive user data.
- ***Improper media sanitization****:* The issue is related to the destruction of physical storage media due to a number of reasons, for example, (a) the disk needs to be changed, (b) the data no longer needs to be there, and (c) termination of service . If the CSP does not sanitize the devices properly, the data can be exposed to risks . Sometimes, the multi-tenancy also contributes to the risk of device sanitization. At the end of the device life cycle, it may not be possible to destroy it as it is in use of some tenants.
- ***Data backup****:* The data backup is also an important issue that needs to be dealt carefully. A regular data backup is needed at the CSP side to ensure the availability and recovery of data in case of intentional and accidental disasters. Moreover, the backup storage also needs to be protected against unauthorized access and tampering.

E. Web application and application programming interface (API) security

The application provided by the CSP is always located at the cloud with users accessing it ubiquitously. One of the important characteristics of cloud applications is that they are not bonded with specific users. Different users may access the same application possibly at the same time. The cloud applications inherit the same vulnerabilities as traditional Web applications and technology. However, the traditional security solutions are not adequate for the cloud computing environment because the vulnerabilities in web application in cloud can prove to be far more devastating than the traditional Web applications. Co-location of multiple users, their data, and other resources makes it much greater issue. The top ten risks in the web applications have been identified by Open Web Application Security Project in 2013 to be the following.

Injection (SQL, OS, and LDAP)

- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Invalidated Redirects and Forwards

The development, management, and use of Web applications must take into consideration the above given risks to safeguard the web applications and users resources. The user and the services in the cloud are bridged by the APIs. The security of APIs highly influences the security and availability of the cloud services. The secure APIs ensure the protected and non-malicious use of the cloud services. An API can be thought of a user guide that describes the details about the CSPs cloud architecture and features. The users build or extend the services using the APIs. The CSPs usually publish their APIs to market the features of their cloud. At one hand, the publishing of APIs helps the users to know the details about the components and functions of the cloud. On the other hand,

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

the cloud architecture to some extent is exposed to the attackers . Therefore, insecure APIs can be troublesome for both the cloud and the users. The vulnerabilities of APIs include weak credentials, insufficient authorization and input-data validation. Moreover, the frequent updates of APIs may introduce security holes in the applications.

F. Identity and access management guidance

The issue of identity management and access control becomes more complex in a cloud environment due to the fact that the owner and resources are in different administrative domains and organization's authentication and authorization may not be exported to the cloud in the existing form . Lack of employee screening and poor hiring practices by some cloud providers may give privileged users such as cloud administrators usually unlimited access to the cloud data. Lack of customer background checks by most cloud providers will help almost anyone to open an account with a valid credit card and email. Apocryphal accounts can let attackers perform any malicious activity without being identified. Lack of security education by people continue to be a weak point in information security . 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. Moreover, unlike the traditional IT setup, the cloud may deal with users of different organization with different authentication and authorization frameworks, at the same time and with the same physical resources. The use of separate authentication and authorization systems for internal organization and cloud may give rise to complex situations over time . The cloud services are elastic and dynamic, the IP addresses are frequently reassigned, the services are started or re-started over shorter periods of time, pay-as-you-use feature allows the users to join and leave cloud frequently. All these characteristics demand that conventional identity management and access control systems are not enough for the cloud environment. There are many issues that can arise in cloud due to weak identity management and access control, for example, denial of service by account lock-out, weak credential reset mechanisms, insufficient authorization checks, cross domain authentication, insufficient logging and monitoring possibilities, weakness of extensible Access Control Markup Language (XACML) messages, and XML wrapping attack.

III. SECURITY COUNTERMEASURES IN CLOUD COMPUTING ENVIRONEMENT

A. Counter measures for communication issues

To secure the communication and network, the CSA guidelines recommend the use of a combination of virtual LANs, IDS, IPS, and firewalls to protect the data in transit. The guidelines also focus on leakage of customers data due to a virtual network and the use of same underlying infrastructure. The CSA recommends the use of aforementioned tools with strict access management policies. Use of virtual devices and conventional physical devices with close-fitting assimilation with the hypervisor is endorsed by the CSA to ensure visibility and monitoring of traffic over the virtual network.

B. Counter measures for Architecture security

Cloud computing security challenges can be handled practically by performing security assessment . An architecture ontology approach for secure cloud computing is defined in various research papers]. The architecture of cloud includes various security components like Access Management, Security API, Network Security and Storage Security. These components embedded in the cloud architecture to provide secure cloud computing

C. Countermeasures for Challenges Inherited From Network Concept

- ***SQL injection attacks:*** Filtering techniques to sanitize the user input etc. are used to check the SQL injection attacks. A proxy based architecture towards preventing SQL Injection attacks which dynamically detects and extracts users' inputs for suspected SQL control sequences has been proposed in various research papers.
- ***Cross Site Scripting (XSS) attacks:*** Various techniques like: Active Content Filtering, Content Based Data Leakage Prevention Technology, Web Application Vulnerability Detection Technology has already been proposed to prevent XSS attacks [31]. These technologies adopt various methodologies to detect security flaws and fix them. A approach that minimizes the dependency on web browsers towards identifying untrusted content over the network has been proposed in [32]

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

- ***Man in the Middle attacks (MITM):*** A few of the important points like: evaluating software as a service security, separate endpoint and server security processes, evaluating virtualization at the end-point have been done to tackle with tis kind of attack in cloud computing [33]. in most of the cases, the security practices implemented (in the organization's private network) apply to the private cloud too. However, in case of a public cloud implementation, network topology might need to be changed in order to implement the security features.
- ***DNS Attacks:*** Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some malicious connection.
- ***Sniffer Attacks:*** A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network [34]. If a hacker is able to get control over the hypervisor, he can make changes to any of the guest operating systems and get control over all the data passing through the hypervisor. Based on the understanding of how the various components in the hypervisor architecture behave, an advanced cloud protections system can be developed by monitoring the activities of the guest VMs (Virtual Machines) and inter-communication among the various infrastructure components [35].
- ***Denial of Service Attacks:*** Usage of an Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks [36]. A defence federation is used in [37] for guarding against such attacks. Each cloud is loaded with separate IDS. The different intrusion detection systems work on the basis of information exchange. In case a specific cloud is under attack, the cooperative IDS alerts the whole system. A decision on trustworthiness of a cloud is taken by voting, and the overall system performance is not hampered.

- Cookie Poisoning This can be avoided either by performing regular cookie cleanup or implementing an encryption scheme for the cookie data. This can be achieved by the scheme introduced. The introduced scheme seem to act reasonably in confronting cookie poisoning attack.

- Distributed Denial of Service Attacks [38] has proposed a swarm based logic for guarding against the DDoS attack. The use of IDS in the virtual machine is proposed in [39] to protect the cloud from DDoS attacks. A SNORT like intrusion detection mechanism is loaded onto the virtual machine for sniffing all traffics, either incoming, or outgoing. Another method commonly used to guard against DDoS is to have intrusion detection systems on all the physical machines which contain the user's virtual machines [40]. This scheme had been shown to perform reasonably well in a Eucalyptus [41] cloud..

D. Counter measures for CAS Proposed Threats

There are also some threats, stated by Cloud Security Alliance, which were explained in the previous chapter. There are some countermeasures to confront these threats. These countermeasures are as follow :

- ***Confronting Abuse and Nefarious Use of Cloud Computing:*** To confront this threat, one should Strict initial registration and validation processes. Another effective measure is Comprehensive introspection of customer network Enhanced credit card fraud monitoring and coordination, and to Monitor public blacklists for one's own network blocks. traffic.
- ***Confronting Insecure Application Programming Interfaces:*** To confront this threat, one should analyze the security model of cloud provider interfaces. Another effective measure is Ensure strong authentication and access controls are implemented in concert with encrypted transmission, to Understand the dependency chain associated with the API. and
- ***Confronting Malicious Insiders:*** To confront this threat, one should Enforce strict supply chain management and conduct a comprehensive supplier Require Specify human resource requirements as part of legal contracts, and assessment. Another effective measure is to transparency into overall information security and management practices, as well as compliance reporting. Another Determine security breach notification processes. useful step to take is to
- ***Confronting Shared Technology Vulnerabilities:*** To confront this threat, one should implement security best practices for installation/configuration. Another effective Promote strong authentication and access measure is to monitor environment for unauthorized changes/activity, and enforce service level agreements for control

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

for administrative access and operations. Other useful steps to take are to patching and vulnerability remediation, and to Conduct vulnerability scanning and configuration audits.

E. Confronting Data Loss/Leakage

To confront this threat, one should implement strong API access control. Another effective measure is to analyze data protection at both design and run time. Other good steps to take protects integrity of data in transit, and Contractually demand Implement strong key generation, storage and management, and destruction practices, and are to providers to wipe persistent media before it is released into the pool. The manager can also contractually specify provider backup and retention strategies.

F. Confronting Account, Service & Traffic Hijacking

To confront this threat, one should prohibit the sharing of account credentials between users and services. Another Employ proactive Leverage strong two-factor authentication techniques where possible, and effective measure is to Understand cloud provider security policies monitoring to detect unauthorized activity. Another useful step to take is to understand cloud provider security policies and SLAs .

In the real word, cloud service providers tend to make use of procedure more that other methods of providing security. This may be because of the fact that some methods are more possible for them to be applied rather that the other ones, due to the economic issues, their inaccessibility to certain tools, or other problems.

IV.CONCLUSION

Cloud computing is a promising and emerging technology for the next generation of IT applications. Although cloud computing has many advantages, there are still many actual problems that need to be solved. The revenue estimation implies that cloud computing is a promising industry. But from another perspective, existing vulnerabilities in the cloud model will increase the threats from hackers. According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible. Data security and privacy issues exist in all levels in SPI service delivery models and in all stages of data life cycle. The challenges in privacy protection are sharing data while protecting personal information. The typical systems that require privacy protection are e-commerce systems that store credit cards and health care systems with health data. The ability to control what information to reveal and who can access that information over the Internet has become a growing concern. These concerns include whether personal information can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited collect, store, and possibly share personal information about users. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. This paper surveyed the key security issues of Cloud Computing being faced today and the challenges and opportunities that it brings for business community . This research paper analyzed what exactly cloud computing security-related issues are, and discussed data security and privacy protection issues associated with cloud computing across all stages of data life cycle. . Future work proposed will help identity management system to achieve more automatic and fast user account provisioning and de-provisioning in order to ensure no un-authorized access to organizations' cloud resources by some employees who has left the organizations. Authorization and access control mechanisms will need to achieve a unified, reusable and scalable access control model and meet the need of fine-grained access authorization. Accountability based privacy protection mechanisms will achieve dynamical and real-time inform, authorization and auditing for the data owners when their private data being accessed.

REFERENCES

[1] Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

[2] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347–358.

[3] Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 93–97.

[4] 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.

[5] Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Springer-Verlag Berlin, Heidelberg.

[6] 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.

[7] Khalid A (2010) Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10), pp 278–281.

[8] 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.

[9] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487.

[10] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA.

[11] Mohammed J. Novel Approaches to Big Data Management. ISSN 2348-1196 (print) International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 1, pp: (96-105), Month: January - March 2015.

[12] Mohammed J. Web and Cloud Security . International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 12, December 2014).

[13] D. AB. Fernandes, L. FB. Soares, J.V. Gomes, M.M. Freire, P. RM Inácio, Security issues in cloud environments: a survey, Int. J. Inform. Sec. 13 (2) (2014) 113–170.

[14] K. Hashizume, D.G. Rosado, E. Fernndez-Medina, E.B. Fernandez, An analysis of security issues for cloud computing, J. Internet Services Appl. 4 (1) (2013) 1–13.

[15] W.A. Jansen, Cloud hooks: Security and privacy issues in cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), 2011, pp. 1–10.

[16] N. Gonzalez, C. Miers, F. Redgolo, M. Simplcio, T. Carvalho, M. Nslund, M. Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing, J. Cloud Comput. 1 (1) (2012) 1–18.

[17] Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia.

[18] Dahbur K, Mohammad B, Tarakji AB (2011) A survey of risks, threats and vulnerabilities in Cloud Computing. In: Proceedings of the 2011 International conference on intelligent semantic Web-services and applications. Amman, Jordan, pp 1–6.

[19] Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1–11.

[20] Jaeger T, Schiffman J (2010) Outlook: cloudy with a chance of Security challenges and improvements. IEEE Security Privacy 8(1):77–80.

[21] 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.

[22] Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35–41.

[23] 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.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

[24] Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security. http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf. Technical report, Helsinki University of Technology, October 2007.

[25] Y. Neng-Hai, Z. Hao, J. Xu, W. Zhang, C. Zhang, Review of cloud computing security, Acta Electron. Sinica 41 (2) (2013) 371–381.

[26] K. Ren, C. Wang, Q. Wang, Security challenges for the public cloud, IEEE Internet Comput. 16 (1) (2012) 69–73.

[27] S.H. Na, E.N. Huh, A broker-based cooperative security-SLA evaluation methodology for personal cloud computing, Sec. Commun. Netw. (2014), http://dx.doi.org/10.1002/sec.1086.

[28] R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, B. Freisleben, Increasing virtual machine security in cloud environments, J. Cloud Comput. 1 (1) (2012) 1–12.

[29] V. Varadharajan, U. Tupakula, Counteracting security attacks in virtual machines in the cloud using property based attestation, J. Network Comput. Appl. 40 (2014) 31–45.

[30] J. Szefer, E. Keller, R.B. Lee, J. Rexford, Eliminating the hypervisor attack surface for a more secure cloud, in: Proceedings of the 18th ACM Conference on Computer and Communications Security, 2011, pp. 401–412.

[31] D. Gollmann, "Securing Web Applications", Information Security Technical Report, vol. 13, issue. 1, 2008.

[32] Ter Louw, M; Venkatakrishnan, V. N.; "BluePrint: Robust Prevention of Cross-Site scripting attacks for existing browsers", 30th IEEE Symposium on Security and Privacy, pp. 331-346, May, 2009.

[33] Eric Ogren, "Whitelists SaaS modify traditional security, tackle flaws", Sep. 17, 2009. [Eric Ogren is the founder and principal security analyst at Ogren Group].

[34] Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, Mounir Frikha, "Malicious Sniffing System Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), pp. 201-207, 2004.

[35] Jenni Susan Reuben, "A Survey on Virtual Machine Security", Seminar of Network Security, Helsinki University of Technology, 2007.

[36] Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing", Journal of Network and Computer Applications, vol. 34, issue 4, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.

[37] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing", 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010.

[38] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment", IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

[39] Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network", IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.

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

[41] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine", ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264,2010.

[42] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment", Sixth International Conference on Information Assurance and Security, USA, pp. 265-270, Aug. 23- 25, 2010.

[43] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus open-source cloud-computing system", in Proceedings of the 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID '09), pp. 124–131, 2009.

AUTHOR BIOGRAPHY

Varun Krishna Veeramachaneni was born in Tenali, Andhra Pradesh, India, in 1991. He received the Bachelor's in Engineering in Computer Science from the JNTU Kakinada, India, in 2013. He graduated in Master's in Computer Science from NewYork Institute of Technology in August 2014. He is about to pursue PhD in Computer Science from MIT's Computer Science and Artificial Intelligence Laboratory. He is presently taking advanced courses in Computer Science from Massachusetts University of Technology (MIT) & Harvard University respectively. In 2014, he worked on various multi-disciplinary projects in Cryptography and Cybersecurity projects as well as on Java and Oracle SOA projects. Presently he is working on his master's research on one of the hottest topics on Cybersecurity. His current research

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

interests include Cyber Forensics, Cryptography, Security and Privacy in Cloud Computing and Big Data, Mobile and Wireless Enterprises, Oracle SOA, and Java. Mr. Varun K. Veeramachaneni is a member of Association for Computing Machinery (ACM) and also a volunteer of STEM program and REACH HIGHER program (Initiative of the First Lady Michelle Obama) at the NYIT, Old Westbury Campus.