A SURVEY ON CLOUD COMPUTING SECURITY CHALLENGES AND SOLUTIONS

Awais Bilal [1], Usman Ahmad [2], Adeel Ahmed [3]

1 School of Electrical Engineering and Computer Science, National University of Science and Technology Islamabad, Pakistan.
2 Department of Computer Science and Engineering, University of Engineering & Technology Lahore, Pakistan.
3 Department of Computer Science, Virtual University of Pakistan.
13msccsabilal@seecs.edu.pk ,usman715@gmail.com, adeelahmed292@gmail.com

***ABSTRACT**: Cloud computing is a new approach to dynamically expand the organizational capabilities, beyond need to spend for infrastructure, hiring new employees and software. Cloud computing paradigm provides easy and on-demand access to a configurable computing resources thorough thin or thick client platforms over the internet. In the recent times, cloud computing has become a fast growing industry. However, as more and more users are tapping into the cloud, security concerns about sensitive data are also arising. Regardless of all the benefits offered by the cloud, people are reluctant to adopt cloud computing, just because of security issues. Security is considered to be one of the primary concerns which is effecting the development of cloud computing. This work presents a survey of security issues in cloud computing environment and specifically talks about the security challenges caused by the service delivery models (SaaS, PaaS and IaaS) of the cloud computing. In this paper, we have also discussed the way of securing cloud computing delivery models along currently available countermeasure against the posed security challenges.*

KEYWORDS: Cloud computing, security challenges, service delivery models, threats, solutions.

1. INTRODUCTION

The advent of cloud computing has remarkably changed the understanding of the hardware architectures, software delivery models and deployment models. The National Institute of Standards and Technology (NIST) has defined cloud computing as 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 [2].

Cloud computing is getting importance and receiving an appropriate attention in all kind of communities; ranges from scientific to industrial. According to a study, cloud computing is the best technology with excelling future in the subsequent years by organizations [6]. Now a days, cloud computing is becoming a craze and most of the organizations are in a try to tap into the world of cloud computing. Cloud computing have the capability to eradicate all the requirements to establish an expensive infrastructure for IT-based solutions and services needed by the industry. It holds the potential to provide extensible IT-based solutions, available through internet for thin or thick client platforms.

In the present day scenario, relatively all small and medium size companies are anxious to enter into the cloud so that they can enjoy a fast application access or can immensely expand their computing capabilities, all at imperceptible charges. Cloud computing offers a lot of benefits such as, fast and easy deployment, scalability, rapid provisioning and de-provisioning, lower cost in almost all aspects, pay-for-use, rapid elasticity of capabilities, on-demand self-services, better resiliency, hypervisor protection, global network access, on-demand security controls, data storage with disaster recovery and ultimately offering business continuity.

In spite of various advantages of cloud computing, yet there are certain serious hurdles to its endorsement. "Security" is one of the most significant hurdles in this respect [5]. Cloud computing offer its services over the internet by combining various computing technologies to provide business applications online, accessible through web browsers. So cloud computing raises many traditional and new security challenges such as vulnerabilities of accessibility, virtualization, web applications, privacy, authentication and authorization. Because of third party's direct access to the data, physical access issues, identity issues, data management issues, data integrity issues, confidentiality and availability issues, provider lock-in, there is a lack of transparency and issues related to the authentication and authorization.

Security is thought to be a prerequisite in consolidating cloud computing as a resilient and realistic solution. Cloud computing not only faces traditional IT related security issues but also encounters new challenges raised by certain features such as virtualization, resource pooling and scalability [8]. Although cloud computing offers better employment of resources, using certain techniques like virtualization and shared infrastructure to facilitate end user, while having certain security risks.

This paper presents different security issues of cloud computing environment, and also discusses about available solutions and the way of securing its delivery models. The rest of the paper is organized as: Section 2 describes about the cloud computing categorization and some basic cloud computing security issues. Section 3 provides details about service delivery models security issues. We present some existing solution in section 4. Section 5 provides the conclusion of this paper.

2. MATERIAL AND METHODS

Cloud computing is a new and a modern way of delivering computing resources and is obviously not a new technology [3]. The term "cloud computing" is comparatively fresh, many is of the view that "cloud" existed long before but in some other forms and referred to by different names [9]. The title cloud computing is derived from the cloud image, which is frequently used to exemplify internet in diagrams. Cloud computing is robustly supported by the virtualization technology which belongs to the mid of last century, for many years available for mainframe computing. In cloud

computing, a host system runs an application which is recognized as a hypervisor, and responsible for creating required virtual machines (VM). Physical systems are simulated so devotedly, that these simulations can run any software, including user applications and operating systems. For storage and processing needs, various physical devices are placed in the datacenters which are independent of the location. Above the hardware level, different layers like software, virtualization and management are combined to offer better server management. Virtualization is a key component of the cloud computing which provide primary features, such as rapid elasticity, resource pooling, and location independence.

2.1. CLOUD COMPUTING CATEGORIZATION

Cloud computing is categorized either on the basis of its deployment models or service delivery models. Fig. 1 shows cloud computing deployment and service models based on NIST framework [2]. Private, public, community and hybrid cloud are deployment models identified for cloud computing, and are described as [4]:

Private cloud: The private cloud always a possession of an organization for its own personal or exclusive use. All cloud resources are devoted to the organization according to its requirements. Private cloud is either hosted locally by an organization or by hiring the services of a third party.

Public cloud: The public cloud is for masses (public or organizations) and is owned by the cloud service provider (CSP). Customers can rent cloud resources according to their requirements and on pay-per-use policy with features like scalability. Google, Amazon, Rack-Space, Salesforce are the current examples of public cloud service providers.

Community cloud: This cloud infrastructure is shared by many individuals or organizations having mutual objectives such as security. Third party services can be hired for the management of the community cloud or can be done by the organization itself. Community cloud can exist on premise or off premise.

Hybrid cloud: The hybrid cloud infrastructure is a result of combining two or more cloud infrastructures in a standardized way. Hybrid cloud infrastructure can include either private, or public or community clouds. The primary objective of this deployment model is to share the burden of other models by providing extra resources (cloud bursting).

Service models in cloud computing includes Software as a Service (SaaS), Platform as a service (PaaS), and Infrastructure as a Service (IaaS) [4].

Software as a Service (SaaS): SaaS provides a range of application running on the cloud infrastructures to the end users without need to bother about technical issues. The servers, operating system, network, storage and all other underlying infrastructures are managed by the CSP, and not the responsibility of the end user. SaaS provided applications are accessible through various devices like laptops, mobile phones, desktops, tabs and workstations.

Platform as a Service (PaaS): PaaS provides capabilities and enable cloud consumers to deploy their applications (either created or deployed) onto the cloud infrastructure, produced by utilizing the tools and programming languages which CSP supports. In PaaS, users have control over the deployed applications, but are not allowed to control the underlying cloud infrastructure.

Infrastructure as a Service (IaaS): IaaS offers infrastructural capabilities to its users including processing, storage, and servers along with other basic computing resources according to their requirements. IaaS facilitates its users to deploy and run software including applications and OS in a flexible environment. In IaaS, end users are also allowed to control the operating system, storage and applications as well as a limited control over the network.

Currently cloud computing is a hot topic, and is considered as a one of the most promising technologies, having the capability of addressing several challenges. Due to its various positives, cloud computing is being used by all kind of organizations including small, medium size to the large corporations (Google, Amazon, Facebook and others).

In Fig.1, the deployment models of cloud computing (private, public, community, and hybrid models) with service delivery models such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are shown. At the bottom layer of the Fig.1, there are some characteristic which are offered by the delivery models such as ubiquitous network, rapid elasticity, measured services, on-demand self-service and multi-tenancy. The security requirements of these basic components of cloud vary according to the use of each specific deployment model. Some of the basic security challenges are relevant to confidentiality of the data; both at rest and in transit, web and the application security, and security issues associated to the acquired services of third parties.

2.2. CLOUD COMPUTING SECURITY ISSUES

Features offered by cloud computing are considered to be both a friend and foe of it, with respect to the security [3]. The advantages offered by the cloud computing are massive.

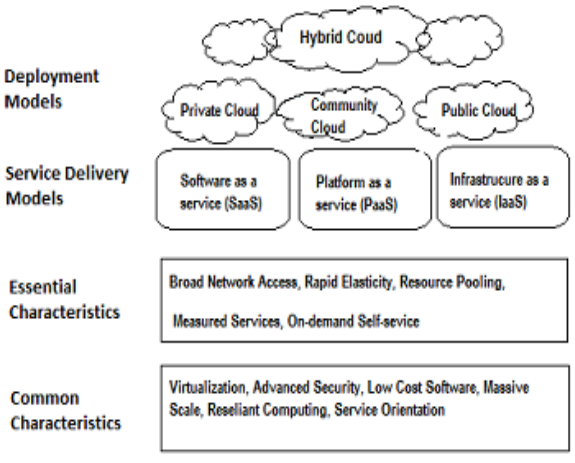

Fig. 1 NIST cloud definition frameework [2]

Although cloud computing introduces more beneficial aspects such as easy and fast deployment, pay-per-use and cost reduction for computing infrastructure, but it also raises some security issues (network security, interface security and security of virtualization layer etc). Security challenges are considered to be addressed at priority, in order to escalate the adoption rate of cloud computing. There are two types of

security challenges which are posed by cloud computing, traditional and the new ones, naturally due to the cloud computing model. Cloud service providers not only need to pay attention to the traditional security challenges, but must also be ready to address the new and emerging security challenges.

Though customary communication system attacks also a threat to the cloud, but cloud computing itself introduces new range of threats that can either make the attacks possible or easier to execute. There is a need to synchronize traditional authentication and authorization applications, used by the organizations to be changed according to the cloud computing environment. Forensic tasks may also become challenging since investigation experts may not have direct access to the computing resources. Availability of the cloud services may also be an issue as, if the cloud services are disrupted, then it effects more users with respect to the traditional paradigm (e.g. disruption of Amazon cloud services). Vulnerabilities of hypervisor and virtual machine may also pose serious problems, especially in a multi-tenant setting, which effects the performance of all the user on the same physical server.

Data outsourcing, lack of access control, virtualization, multi-tenancy, and internet dependency are the security challenges related to risk areas. Due to the specific structure of the cloud computing such as large scale resources, location independence and its virtualized environment, traditional security mechanisms are not sufficient for the current cloud models [7]. Most of the security controls for the cloud computing are similar to the security controls for an IT framework. Most of the conventional security measures are applicable to address the security challenges of cloud. But cloud computing poses different threats to the business than the traditional, because of the service models and technologies used for the operational models. Cloud service providers must satisfy the security concerns raised by the end users and provide evidence of how they can achieve what they claim for (through service level agreements), and also demonstrate compliance to the auditors.

3. SECURITY ISSUES IN DELIVERY MODELS

Software as a service, Platform as a service and Infrastructure as a service are the three delivery models through which cloud computing offers its all range of services. These delivery models are termed as, SaaS, PaaS and IaaS which are responsible to provide software as a service, platform for applications and infrastructure resources to the end user. Cloud service delivery models demand specific security arrangements in cloud setting. IaaS is at the bottom of all the service models, PaaS is on the second tier, just above the IaaS, and SaaS built upon the PaaS. The features are passed on to each delivery model, same as the security hazards. There is a trade-off for each delivery model in terms of features and security. If service provider ensures the security of lower layers only, then it becomes the responsibility of the ender user to take necessary security measures for the upper layers.

According to a survey by Cloud Security Alliance (CSA) and IEEE, all kind of organizations are keen to enter cloud computing but security creates certain concerns in their mind. It also mentions that cloud computing is modeling the IT industry in new dimensions but lack of compliance is having a considerable effect on its wide scale adoption [10]. Organizations moving their business resources to the cloud, would like to investigate the privacy and confidentiality issues in detail. Although it is not impossible to certify the security of business applications in the cloud, but it remains a challenging task. Because each cloud service delivery model (SaaS, PaaS and IaaS) has different security issues (as discussed below).

3.1. SOFTWARE AS A SERVICE (SaaS) SECURITY ISSUES

In SaaS delivery model, the end user has a relatively less control, and depends on the service provider (CSP) for the effective security actions. Provider is responsible for the data security, and ensures to keep every user's data separate and protects its privacy and confidentiality. The vendor may rent the services of third party to host its applications or may have private servers. The service provider may replicate data to the other locations as well, to ensure the availability. Since in traditional models, almost all the data reside within the controlled boundaries of an entity, contrary to the SaaS model. So this lack of control creates confusion on the client side, about their data storage and security in the SaaS model.

Fig. 2 depicts the important aspects that must be addressed to ensure data security in a typical SaaS vendor model. Following security measures must be considered in SaaS environment.

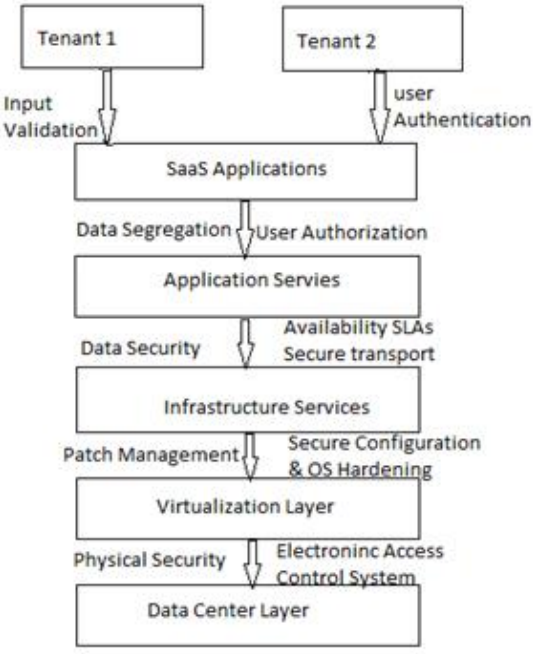

Fig. 2 Security for SaaS Stack [27]

3.1.1 DATA SECURITY

Data security is always an important concern, but it becomes challenging when it comes to SaaS model. In a traditional application model, organization's data resides in its own boundary, relying on its security policies. But in the SaaS model, the sensitive data resides on the provider's end, outside of the user's boundary. So the provider must employ

extra security controls to ensure data security against application vulnerabilities and malicious insider attacks. Cloud providers such as Amazon, allows secure, logged and auditable access to the host with a specific business need to their administrators, and they do not have access to the customer instances. While the data is stored in plain by default, however user can encrypt their data before uploading. Following security elements must be considered to prevent the unauthorized data access by the malicious users:

- Access control vulnerabilities
- Insecure storage location
- Cross site scripting (XSS)
- SQL injection
- Cookies and hidden field manipulation
- Configuration issues

3.1.2 DATA TRANSPOTATION SECURITY

In a SaaS model, client shares confidential data with SaaS application for processing, then after processing this sensitive data, it is stored at the CSP's specified storage place. In order to prevent data leakage, there is a need to secure the network communication. Man-In-The-Middle (MITM), port scanning, IP spoofing and packet sniffing are the potential threats to the data transportation which can be catered by network security techniques such as secure socket layer (SSL) and transport layer security. However, several network configuration vulnerabilities may encourage malicious users to exploit them. The following security assessments are capable of ensuring the credibility of the SaaS provider.

- Network penetration
- Packet analysis
- Session hijacking or session management vulnerabilities
- SSL trust configuration issues

Any exploit of the founded vulnerability can allow malicious user to effect the confidentiality and integrity.

3.1.3 DATA LOCALITY

In SaaS, consumers process their sensitive data by utilizing applications provided by SaaS vendors, however without having any knowledge of data storage location. In certain situations, data locality may be a great concern, because different countries in the world have their own laws about the data privacy and confidentiality. Despite of the laws problem, there is another problem of jurisdiction that under whose jurisdiction data falls at the time of investigation. A SaaS vendor must ensure the reliability of data location to the customers.

3.1.4 DATA SEGREGATION

Multi-tenancy is an important characteristic of cloud computing. It tolerates several users to store their sensitive data by utilizing SaaS applications [11]. In this case, data location of various users will remain same. In this situation, one user becomes able to lean into the data of other users by hacking through the application vulnerabilities or by compromising the SaaS system. An attacker can write a piece of malicious code and insert it in to the application. If the application does not perform input filtering and process the code without proper verification, then this will make other user's data vulnerable to various attacks. An attacker can exploit application vulnerabilities to avoid security measures to have an access to the neighboring tenants. A SaaS provider can perform following assessments to validate the strength of data segregation.

- SQL injection bugs
- Input filtering
- Storage vulnerabilities

3.1.5 ACCESSIBILITY

SaaS applications are accessed over the internet via web browser through thin or thick client platforms such as desktops, tabs, mobile phones, laptops etc. But it also opens the SaaS applications to certain security threats. Accessibility issues also arise due the user provided security policies. Accessibility issues mainly related to the threats such as network vulnerabilities, OS vulnerabilities, application vulnerabilities, and insecure marketplace.

3.1.6 WEB SECURITY

SaaS applications are available over the internet and usually operate behind the firewall. Its network based access and management enable users to access applications remotely though the web. Thus security flaws in the web applications may become a root cause create certain vulnerabilities in the SaaS application. In such cases, there is a possibility that this vulnerability will have a negative impression on every user who is using cloud. This security challenge is more alike to the other web-based technologies. However, traditional network security solutions will not be able to provide an effective defense and do require defense at application level.

As web applications and SaaS together provide services to the customer, so most of the security challenges related to the web are also applicable to the SaaS applications. Following are some of the top security challenges:

- SQL and OS injection flaws
- Cross site Scripting
- Transport layer security issues
- Direct object reference issues
- Redirect and forward issues

3.1.7 AVAILABILITY

One of the challenges, SaaS applications are facing, is round the clock availability of the provided services. To ensure availability and scalability, there is a need of certain changes at the application as well as at the infrastructural level. Resiliency against attacks like Dos and hardware/software failures must be considered from the design phase of the application. SaaS applications availability can be improved by performing following assessments,

- Authentication flaws
- Session management vulnerabilities

3.1.8 BACKUPS

SaaS providers ensure data backups at regular basis for business continuity and disaster recovery purposes. Encryption techniques are also used to protect data backups against accidental leakage. In case of certain SaaS providers such as Amazon, data is not stored in the encrypted form (in Simple Storage Service S3). So it is recommended for the customers to upload data in the encrypted form. The security of the backups can be validated by performing following assessments,

- Insecure storage
- Insecure configuration

Exploitation of the detected vulnerabilities may lead to the unauthorized access to the data stored in the backups.

3.2 PLATFORM AS A SERVICE (PaaS) SECURITY ISSUES

PaaS enables the development of cloud centered applications on top of it, without the need to spend high cost on buying underlying infrastructure. In PaaS, the user may have some control to build application, but the security of the underlying resources below the application is still under control of the provider. So PaaS provider is responsible to safeguard the data between applications. Attack on the PaaS application effects the security of two layers: firstly the security its own, and secondly the security of the deployed application [12]. Just like SaaS, PaaS also poses challenges such as data security and some other, that are describes as following:

3.2.1 THIRD PARTY RELATIONSHIP ISSUES

PaaS provides cloud supported programming languages as well as third party web service units like mashups [12]. Mashups integrate two or more source units into a one element. PaaS model inherits feature of mashups as well as security challenges such data and network related issues. Thus PaaS customers rely on the security measures provided by the PaaS vendor, and web service provider.

3.2.2 APPLICTION DEVELOPMENT LIFE CYCLE

From the application development point of view, it is difficult to develop secure applications for the cloud, because the way application changes in the cloud, effects the security and system development life cycle [16]. There is a need to ensure flexibility in the application development life cycle as frequent changes may occur in the in the PaaS environment. Besides flexibility, developers must ensure that, any changes in PaaS should not create security problems for the applications. With the knowledge of secure development, developers must also know the data location complexities that may create security issues such as privacy.

3.2.3 UNDERLYING INFRASTRUCTURE SECURITY

In PaaS, user cannot access the underlying infrastructure, so it is the duty of the provider to secure the underlying resources. Developers have the capability to secure their applications, but do not have guarantee that the provided tools are also secure. Data security depends on the measures taken by the provider while it is being processed, transfers, and stored.

3.3 INFRASTRUCTURE AS A SERVICE (IaaS) SECUIRTY ISSUES

IaaS infrastructure is capable of providing range of computing resources namely network, processing power, servers and storage in a virtualized form [16]. In IaaS, customers enjoy better control and management of the running software. IaaS customers have relatively improved control on the security issues, if compared to SaaS or PaaS models, as they can control the software and can configure the security policies. However, the security of underlying infrastructure such as network and storage is still the responsibility of the provider. Some of the IaaS related security issues are:

3.3.1 VIRTUALIZATION

With virtualization, users may enjoy features like create, copy, and share, migrate and roll back

Table 1: Summary of security challenges and solutions of cloud computing

Level	Service Level	Security requirements	Threats	Solutions
Application level	Software as a Service (SaaS)	Privacy in multi-tenancy Data confidentiality Access Control Network Security Application security Availability	Session hijacking Data modification in storage. Data interruption Traffic analysis Impersonation Data modification while in transit Interception Privacy beaches Injecting malicious data	Identity and access management guidance [19]. Digital signatures. Encryption. Use of SSL/TLS techniques. SLAs
Virtual Level	Platform as a Service (PaaS) Infrastructure as a Service (IaaS)	Application security Access Control Image security Virtual machine security Communication security Data security both in storage and in transit Hypervisor security Compliance and audit	Programming bugs Software modification Software interruption Impersonation Session hijacking Traffic flow analysis Network/connection flooding Dos/DDos	Web application security. Digital signatures. PALM [21]. Encryption techniques. User input filtering. Service level agreements
Physical level	Physical datacenters	Legal use of cloud computing Hardware security Hardware reliability Physical access control Computing resource protection	Hardware theft Natural disaster Misuse of infrastructure Networks attacks Interruption of hardware DDos	Door locks and security guard Monitoring mechanism (CCTV Cameras) Secure location selection Separation of duties Use of firewalls and IDS

virtual machines (VM), and are allowed to run various applications [13]. However, it also opens new doors for malicious user, due to the addition of an extra layer which need security.

3.3.2 HYPERVISOR SECURITY

Hypervisor isolates virtual machines, so if it is compromised then there is high possibility that its VMs may also be compromised. Hypervisor resides at the lower level and manages the VMs, and may also have security holes. For better security controls, it is recommended to keep the hypervisor simple and small. Virtualization allows VMs to migrate between physical servers to improve its performance capability. This feature also poses some security challenges like an attacker can take a migrating VM to the malicious server by compromising the migration module. This migration of the VM may further lead to the security issues such as data integrity and data confidentiality.

3.3.3 SHARED RESOURCES

In virtual environment, VMs share some resources such as memory and CPU etc. This sharing in the virtualization may affect the security of each VM. Shared resources may cause security issues such as covert channel communication and information stealing from the other VMs. In this scenario, a compromised VM can monitor shared resources without any knowledge of the hypervisor.

3.3.4 VIRTUAL NETWORKS

Resource pooling allows sharing of network components among different tenants. Since it is obvious, that recourse sharing permits cross-tenant attacks. VMs interconnectivity increases through virtual networks which is an important security issue in cloud environment. From the security point of view, there is a need to link each VM with its host through a dedicated physical channel, but majority of hypervisors use virtual networks. Virtual networks are prone to sniffing and spoofing [15].

3.4 NON-TECHNICAL SECURITY ISSSUES IN CLOUD

In the previous sections, we have mainly focused on the technical security challenges which are specific to service delivery models of the cloud computing. However, there are some other security issues that are common. There is a strong desire to address these issues, as it can potentially effect the performance of cloud computing and its infrastructure. Some of these challenges that the cloud security alliance (CSA) has highlighted are following:

Poor pre-employment screening and hiring practices: Usually employees of cloud computing environment do not pass through an effective screening process. There is clear gap between background screening performed by the provider, and the privileges that employees have such as administrators [20].

Insufficient user background information. Lack of user background information required during the authentication process also open doors for the attackers. Most cloud service providers allow any person with a valid credit card and email ID to use the services of cloud. This allows attackers to take advantage of cloud capabilities to perform their malicious activities, with anonymity.

Lack of security knowledge: In information security, people are considered to be a weakest links. This is due the lack of security education and practices. In cloud computing environment, this factor poses a greater challenge, due to the presence of various users at the same place and same time.

4. RESULTS AND DISCUSSION

There are various research groups and organizations who are working for the security solutions of cloud computing. One of them is a Cloud Security Alliance (CSA), which is a non-profit organization and is working to secure the use of cloud computing. There are some other organizations and groups such as Open Grid Forum and Open Web Application Security Project (OWASP), which are also working on cloud computing security challenges [17, 18].

4.1. SECURITY SOLUTIONS

The following are some solutions against several security issues, proposed in this and other research works:

4.1.1 SECURING SOFTWARE AS A SERVICE (SaaS) MODEL

Confidentiality of the data is at the top of the priority list for every company while hiring the services of the third party. Cloud service providers (CSP) must not only match but should exceed the security requirements to win the trust of the clients.

As mentioned above in SaaS security issues, data is exposed to certain threats such as Access control vulnerabilities, Insecure storage location, Cross site scripting (XSS), SQL injection, packet sniffing, Session hijacking or session management vulnerabilities, SSL trust configuration issues while at rest or stored at a particular location. Following are some of the areas which can help CSPs to secure their customer's data. These points may also act as guideline for the customers to gauge the level provided security by the CSP.

Protection of authentication credentials: Authentication refers to the process of validating user's identity, and after successful authentication a user is granted access to the system or data for which he is authorized to. Security of the authentication credentials is important and there should be a secure way to store them. From security perspective, it is recommended to store these credentials in a separate server, other than the application server. So customer may ask CSP that, how authentication credentials are stored and managed?

Encryption of user files: This is directly related to the user files that are stored on the provided location by the CSP. CSP may have protected the location but has no value if the customer files are recognizable by the layman. There is need of strong encryption algorithms to convert information into unintelligible form while data is at rest. Customers may ask CSP that, what encryption and storage mechanism are used?

How multi-tenancy is handled? In cloud computing multiple tenants or customers share the same application but their data at the backend is segregated. Multi-tenancy can be exploited by the malicious users to lean into the data of other users which is threat to the confidentiality of the data. Even multi-tenancy is one of the important and necessary features of cloud computing but there is a need to ask about the architecture of the database. The customer should ask the CSP that, how data is ensured to be separated among all tenants.

Accessibility of user files: Even if CSP has implemented all the security mechanism but he himself has access to the confidential data then the provided security has no value. It is recommended for the user to sign legal documents about the accessibility of data. They should clearly mention that who, how and under what conditions one can access data. CSP's privacy policy should be read thoroughly and discuss in detail with the CSP.

File deletion and storage media destruction: CSP usually retain user deleted files for few days for recovery purposes. As it has the advantage of recovering the data but on the other hand this may also be recovered for malicious purposes. Here another problem can be of how storage media is replaced? Whether old drives are disposed off properly or just thrown into the bin. In this regard CSP's privacy policy plays an important role.

Logging mechanism: Logging plays a vital role in determining about the system accessibility. It provides information about who, how and at what time and from where system was accessed. Logging can be done locally as well as on the centralized locations. Customers should also conquer about the access rights to the logs.

Firewalls and intrusion detection systems: Firewalls protect the system from outside invaders but it depends on what type of firewall(s) is being used. Some common firewalls which can be used; such as packet filtering firewall, packet inspection firewall and application level firewalls. IDS also help to determine if any unusual activity is performed.

4.1.2. SECURING PLATFORM AS A SERVICE (PaaS) MODEL

PaaS provides the facility of deploying applications without bearing expenses for buying and managing the underlying infrastructure. PaaS offers certain features such as application design and development, testing and deployment. Cloud users need to ask following points before going into the cloud services and must sign service level agreements accordingly,

- How CSP will ensure the business continuity planning and disaster recovery?
- How CSP will ensure a secure software development life cycle (SDLC)?
- Customers should assess that whether they can be got affected by the vendor lock-in or not? If yes, then up to what extent?
- To analyze the adequate provisions in the service level agreements
- Perform risk assessment of adopting the services of PaaS.

4.1.3. SECURING INFRASTRUCTURE AS A SERVICE (IaaS) MODEL

People are now keen to adopt economically efficient solutions for their organizations by enjoying the services of IaaS. But before adopting IaaS solutions there is a need to consider certain security issues of it. These security issues may vary depending on the usage of the deployment models of cloud computing. For example in private cloud user enjoy full control of it but on the other side if someone is using public cloud then their control limits to the virtual machines and on the services running on them. In both cases, users must seek answers to the following questions,

- How the leakage of the data is protected and its usage is monitored?
- How secure are their authentication and authorization mechanism are?
- How penetration into the infrastructure is handled?
- What is the level of data encryption (end-to-end or not?

4.1.4. CURRENT SOLUTIONS FROM RESEARCH WORK

Some of the currently practiced solutions for to cater certain attacks are as follow:

An identity and access management guidance has been presented by the Cloud Security Alliance (CSA), which recommends certain practices such as centralized directory, identity and access management, role based access control, separation of roles etc. This guidance stands as a countermeasure against threats like service or account hijacking [19].

Cloud data passes through three steps, i) transfer, ii) store, and iii) process. Several encryption procedures can help to improve the security of cloud data during the transfer, or at rest in storage location. Some of the approved encryption schemes such as AES, SSL can be used to secure cloud data. Through the use of encryption schemes, data leakage type threats can be resolved.

Web application firewalls are also used as a solution against web attacks. Web application firewall routs all the traffic though itself to detect security threats.

Data in the processing phase can be secured by isolating resources. In this technique, processor cache is isolated in VMs, and this virtual cache is isolated form the hypervisor cache [22].

IP spoofing can be prevented by using encrypted protocols, where possible, as suggested in [25]. This work also talks about the prevention of ARP poisoning, by linking ARP table changes with the root access.

For data privacy and control issues, tight service level agreements are required.

The solution proposed in [23]; make use of asymmetric cryptography in connection with SSO and LDAP, to safeguard the confidentiality, authentication and integrity of the involved data as well as communication.

Protection aegis for live migration (PALM) of virtual machines (VMs) suggests a safe live migration of the virtual machines by maintaining their integrity and privacy. PALM ensures integrity as well as privacy at both stages, at the time of migration and afterwards. According to its results, it bears a minor overhead of en/decryption processes with respect to downtime and migration time. [21].

Although cloud computing leverage web technologies for its implementation, it also put it in front of new security issues. Security web services standard has talked about the way to secure communication between applications while ensuring CIA model and authorization [24]. Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML), XML digital signature and encryption, WS-security and Key Management Specifications (XKMS) and others are available security standards [26].

5. CONCLUSION & Future Work

Cloud computing is a relatively novel, emerging and a promising technology that helps small and medium size organization to save infrastructure or operating cost while boosting up their capabilities. Although it offers extreme benefits, but it also inherits a number of security challenges from the adopted technologies. Cloud computing is being used in all kind of organizations, from small to large scale, but still security controls are immature. At this time, security is no doubt a major barrier in uprising the acceptance rate of cloud computing. Organization should understand the security risks that cloud computing may pose too their sensitive organizational data. This paper talked about various security challenges, that an organization can consider before entering into the world of cloud computing. It also discussed some of the suggested solution in the research work that may help in improving the security situation of cloud.

We have given summary of the cloud computing and its categorization. Then we described about the security challenges in the cloud computing environment, including both traditional challenges which are also applicable to cloud, and various fresh challenges which arises due to the cloud. Specifically, we described security issues for service delivery models (SaaS, PaaS, and IaaS), who's security requirements fluctuate according to the model. Network security, application security, and the web security are biggest security issues. Virtualization, which is one of the important parts of the cloud, is also a key security concern for the customers. Brief overview of the basic security solutions is also provided. Currently several research groups are proposing different security techniques which are immature. There is a need to reshape traditional security solutions to work with cloud as well as of new security techniques to secure cloud computing.

REFERENCES

[1] Mell Peter, Grance Tim, *Effectively and securely using the cloud computing paradigm*; 2011. http://csrc.nist.gov/groups/SNS/cloudcomputing/cloudcomputing- v26.ppt

[2] National Institute of Standards and Technology, *The NIST definition of cloud computing; 2011*. <http://www.nist.gov/itl/cloud/upload/cloud-defv15.pdf>

[3] Catteddu D, Hogben G, *Benefits, risks and recommendations for information security,Tech. rep., European Network and Information Securit Agency, enisa.europa*.eu/act/rm/files/deliverables/clodcomputing-risk-assessment, 2009.

[4] Cloud Security Alliance, *Security guidance for critical areas of focus in Cloud Computing* V3.0..Available:https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011.

[5] KPMG 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

[6] Gartner Inc Gartner, *the Top 10 strategic technologies for 2011,* Online Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed 04-Aug-2014

[7] Li W, Ping L, *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, 2009.

[8] Chen Y, Paxson V, Katz RH, *What's New About Cloud Computing Security?*, Technical Report UCB/EECS-2010-5, University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html. Accessed 06-Aug-2014.

[9] Rong, C., Nguyen, S.T., Jaatun, M.G.: *Beyond lightning: a survey on security challenges in cloud computing*, Comput. Electr. Eng. .doi:10.1016/j.compeleceng.2012.04.015 Available online 19 May 2012

[10] Cloud Security Alliance, *Survey by IEEE and CSA details Importance and urgency of cloud computing security standards*, Available:https://cloudsecurityalliance.org/media/news/survey-by-ieee-and-cloud-security-alliance-details-importance-and-urgency-of-cloud-computing-security-standards/. Accessed 08-Aug-2014

[11] S. Subashini, ,Kavitha, V., *A survey on security issues in service delivery models of cloud computing*, Journal of Network and Computer Applications, vol. In Press, Corrected Proof.

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

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

[14] Cloud Security Alliance, Security guidance for critical areas of Mobile Computing. Available:https://downloads.cloudsecurityalliace.org/initiatives/mobile/Mobile_Guidance_v1.pdf, 2012.

[15] Xiaopeng G, Sumei W, Xianqin C, *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, 2010.

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

[17] *Open Grid Forum.* https://www.ogf.org/ogf/doku.php

[18] *Open Web Application Security Project (OWASP)*, https://www.owasp.org/index.php/Main_Page

[19] Cloud Security Alliance, *SecaaS implementation guidance, category 1: identity and Access management.* Available:https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf, 2012.

[20] Cloud Security Alliance, Top Threats to Cloud Computing V1.0.Available:https://cloudsecurityalliance.org/research/top-threats, 2010.

[21] Zhang F, Huang Y, Wang H, Chen H, Zang B, *PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In: Trusted Infrastructure Technologies Conference*, APTC'08, Third Asia- Pacific, IEEE Computer Society, Washington, DC, USA, pp 9–18, 2008.

[22] Raj H, Nathuji R, Singh A, England P. *Resource management for isolation enhanced Cloud services*, In:Proceedingsofthe2009 ACM workshop on cloudcomputing security, Chicago, Illinois, USA, 2009, p.77-84.

[23] Zissis, D. and Lekkas, D., *Addressing cloud computing security issues*, Future Generation Computer Systems. doi:10.1016/j.future.2010.12.006, 2011.

[24K Hashizume et al., *An analysis of security issues for cloud computing*, Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013.

[25] Basta A, Halton W., *Computer security and penetration testing*, Delmar Cengage Learning 2007.

[26] Fernandez EB, Ajaj O, Buckley I, Delessy-Gassant N, Hashizume K, Larrondo- Petrie MM, *A survey of patterns for Web services Security and reliability standards*, Future Internet 4(2):430–450, 2012.

[27] *Securing SaaS Applications*, http://www.infosectoday.com/Articles/Securing_SaaS_Applications.ht
m. Accessed 09-Aug-2014.