International Journal Of

Recent Scientific Research

ISSN: 0976-3031

Volume: 7(5) May -2016

REVIEW ON CLOUD SECURITY ISSUES: CHALLENGES AND SOLUTIONS

Najeeb Ahmad Khan., Tamanna Siddiqui and Riaz Ahmad

THE OFFICIAL PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH (IJRSR)
http://www.recentscientific.com/ recentscientific@gmail.com

ISSN: 0976-3031

Available Online at http://www.recentscientific.com

International Journal of Recent Scientific Research
Vol. 7, Issue, 5, pp. 10846-10853, May, 2016

International Journal of Recent Scientific Research

Review Article

REVIEW ON CLOUD SECURITY ISSUES: CHALLENGES AND SOLUTIONS

Najeeb Ahmad Khan., Tamanna Siddiqui and Riaz Ahmad

Department of Computer Science, Aligarh Muslim University, Aligarh (UP), India

ARTICLE INFO

Article History:

Received 05th February, 2016
Received in revised form 21st March, 2016
Accepted 06th April, 2016
Published online 28th May, 2016

Keywords:

Cloud Computing, Security, Service Model and Development Security

ABSTRACT

In the present day, Cloud computing is a growing recent computing style for providing computing service contracts. A number of researchers realize that Cloud computing is likely to redesign the IT market as a mutiny. Cloud computing generate multi-level virtualization and abstraction via useful integration of type of computing, storage space, data, applications along with additional assets , users who want to use strong computing and storage space of cloud computing only have to connect with the network . Within this paper, review of cloud computing models have been presented. The objective of this paper is to present challenges of cloud security issues of cloud computing models and to suggest appropriate solution to handle those issues.

INTRODUCTION

Several public, the word cloud computing includes the sense of a buzzword. But cloud computing is not a buzzword any more than the word the Web is. Cloud computing is the progress of various technologies that work together to modify an organization's strategy to building out an IT infrastructure. Cloud computing is a brand new pattern of computing model which comes into limelight after parallel, distributed, grid computing and so on. Cloud computing is just one of those Web-based computing, where shared assets, data storage space, data and details are provided computers and various other devices on-demand access. It is definitely clear that, from 2009, the cloud is known as the most well-known space in computer science and engineering technology for IT industry, Amazon, Google, Yahoo and other Web based service, IBM, Microsoft together with other IT providers have put forward their unique cloud computing method, different telecom operators will also be have place a large deal of interested on cloud computing, the highly good deal of cloud computing platform becomes the primary aim of the IT market. Google states that due to the using cloud computing technology, its working out expense is only competitors 1/100, the storage expense is only competitors 1/30. So, cloud computing can be very useful for business point.

Most of the time, cloud computing creates privacy concerns for the reason that the service giver can access the data and information that is definitely in the cloud system. It could accidentally or deliberately alter or even remove details. A lot of cloud givers can discuss information with third parties if required for reasons of law and order even without a justification. Which is allowed in their privacy plans which users have to permit just before they make use of cloud services. Solutions to privacy can include policy and laws as well as end users' options for exactly how information is saved. Users can encrypt data which is processed or saved within the cloud to avoid unauthorized access. The top three risk in the cloud computing are Insecure Interfaces and API's, Data Loss and Leakage, and Hardware Failure by the cloud security which accounted for 29%, 25% and 10% of all cloud security. Microsoft is dedicated to providing a cloud trust. We think there exist some appropriate areas you need to know about cloud security.

- Security possible choices and features easily obtainable in the cloud.
- Providing level of privacy and control of your data.
- Focusing on market compliance rules.
- Making the most of hybrid features without affecting the advantages of the cloud.

Cloud Models

There are two basic models in cloud computing such as Service models and deployment models.

Service Models

The services in the cloud, also run and managed by a cloud service provider. Cloud computing it's depending on the offer of providers, we listed three types of service [25][2]:

**Corresponding author: Najeeb Ahmad Khan*
Department of Computer Science, Aligarh Muslim University, Aligarh (UP), India

Infrastructure as a Service (IaaS) -Users can use directly detail of infrastructure such as security, networks, storage, hardware etc. to offer computer application environments with an asset usage-based pricing model. IaaS are usually offering some other resources like as virtual machine, load balancers, virtual LANs, and IP addresses.

Platform as a Service (PaaS) -The end-users are provided a platform that can be used to build applications. PaaS users does not manage cloud infrastructure including storage or network. It also offer high level development software, test and consumer applications.

Software as a Service (SaaS) - Known as on- demand software package which is regularly charge on a pay per end user time. In this mode, different types of utility applications i.e. accounting, spread sheet and word processing etc. are offered as service to clients. The SaaS also includes Google /mail, Google Drive etc.

Hybrid Cloud is a combination of two or more than two clouds (private + public). Services can be consumed by anyone who pays for it. It takes advantage from both of those deployment models. Such as, an organization could keep very sensitive information about their private cloud and make use of the public cloud for managing large traffic and challenging situations.

Cloud Security In these days cloud security is the most important issue to be handled. Data is at high risk, when security and safety situations are not given correctly for data function and transmissions [24]. Since cloud computing can provide a potential for an amount of consumers to gain access to the saved data there is an opportunity of obtaining high data risk. Most powerful security methods need to be implemented by identifying security issue and clarifications to manage these types of issues [2] [3]. The most important factor, how to makes data secure and privacy which is shown as figure 1

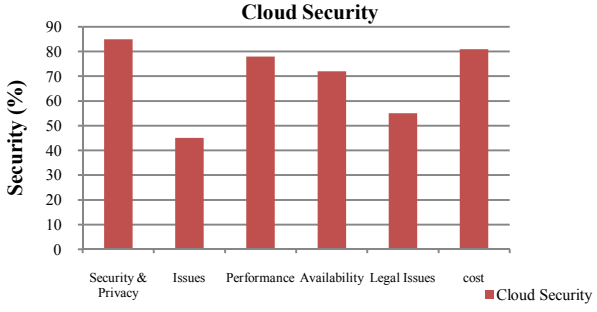
Table-1 Services of SaaS, PaaS and IaaS

Parameter	PaaS	IaaS	SaaS
Paradigm Shift	License purchasing	Infrastructure as an asset	software as an asset
Who use it?	Creator and Deploys	System Manager	Business End User
Why use it?	Provide application and services for users	Provide platform for service application test, development, integration and deployment	To Complete Business Task
When not to use it.	N/A	If capital budget is more than operating budget.	N/A
What Services Are Available?	Service and application test, integration and deployment, development.	Virtual machine, Message queue, memory, Network, Storage, operating system, CPU, backup service	Email, Office, Wiki, Blog, CRM Website testing, Automation, Virtual Desktop…..
Managed By Vender	Runtime, O/S, Servers, Networking, Storage space, Middleware, Virtualization.	Servers, storage space, Networking, virtualization.	Runtime, Applications, Data, virtualization, Servers, storage space, middleware, Networking.
Key Terms	Solution Stack	Hypervisor, Resource pooling, Grid, Utility and Multi-tenant computing.	Thin client, Client-server application
Common IaaS Use-Case	Reducing utilization rates of an application's time-to-market and Rises developer productivity	Extends current data center infrastructure for temporary workloads	Replaces traditional on-device software
Technology Analyst Example	Gartner- Richard Watson, Eric Knipp, Yefim Natis Forrester- Stefan Ried, John Rymer	Gartner- Kyle Hilgendorf , Drue Reeves , Gregor Petri , Tiny Haynes Forrester- Hammond, James Staten	Gartner- Bill Pray Forrester- Amy DeMartine
Characteristics	Uses cloud infrastructure , designs for agile project management plans	Mostly platform independent, pay by usage, self-scaling, infrastructure expenses are shared and minimized, SLA.	SLAs , UI using narrow client applications , communication via APIs stateless , cloud components , semantic interoperability
Advantages	Streamlined version deployment	Lower capital expense on h/w and user assets, reduced ROI risk, cheap barriers to entry, efficient and automated scaling.	Eliminate expense on computer software and development assets , minimize ROI threat , latest and iterative updates
disadvantages	Centralization requires new/different security steps.	Business performance and efficiency mostly depends on the vendor's skills, centralization needs new/different security steps.	Centralization of information and data needs new/different protection steps.

Deployment Models The cloud area has commonly used following three cloud deployment models:

Private Cloud is the idea of cloud computing on a private network. The cloud system is managed totally for an organization. Normally it is handled by the organization or a third parties and may occur on premise or off premise. The serious issue using this type of deployment model is that the users have large cost as they simply have to purchase the infrastructure to execute the cloud as well as have to handle the cloud itself.

Public Cloud is the easiest form of cloud infrastructure that is designed for public end user. The services are supplied to individuals and organizations. Public cloud consumers are by default addressed as irresponsible.



One out of the threats that citizens notice is usually that providers need to handle possibly millions of users and this features an issue (Ohlman, Eriksson, & Rembert, 2009). Privacy is necessary for IT market, especially when individual's public details or very sensitive details are being

saved but it surely is not yet completely known about whether the cloud computing system should be able help the collecting of sensitive details without making organizations liable from cracking level of privacy rules. Cloud providers consider encryption is definitely the key and can help with a number of the security issues. Encrypting is not always full signs for securing data, there can be times when little errors arise as well as the information should not be decrypted leaving the data bent and fallow for users and the cloud service provider. And also, the multi-tenancy model and the pooled computing assets in cloud computing has introduced novel security issues that need novel strategies to attempt with [3] [4]. There are two new security issues for creating in multi-tenancy model.

- A shared resource on the similar actual physical machine invites unexpected side channels between a risky resources along with an ordinary resource.
- Standing fate-sharing will very harm the reputation of several outstanding cloud "citizens" who occur to, unfortunately, share the computing assets with their fellow tenant - an infamous user with a lawbreaker mind.

Security Aspects to Focus on Cloud Computing

Confidentiality

It is actually the region of making sure a personal data are presented private, secured and restricted anywhere from around not authorized users. Data encryption is one of famous techniques of safety and security before shifting the data into the cloud.

Authentication and Authorization

It's the process to provide verifying the identification of any individual and exactly what an individual is authorized to do--is the following phase. In authentication the developing blocks related to an electric idea or file is properly identified.

During this process the data is secure and safe from accidental or risky modification.

Non-repudiation

It describes the capability to make sure a party to an agreement is not able to reject the authenticity of their signature on a document or the transmitting of a massage/an email that they previously started.

Privacy and control

Privacy is a highly important problem for cloud computing, each and every with respect to lawful agreement and user trust require to be taken into consideration at every single step of design. Control is the best way to manage the utilization of the system, like applications, infrastructure and data.

Audit

The facility for a business enterprise to monitor exactly what applications users are using (and when) is a situation from both a security and regulatory point of view. It might be included as an extra layer above the virtualized process system managed on the virtual machine to give services for observing how it happened for such type of situations as well as other factors that effected the system availability needs to be audited.

Compliance

Compliance issues occur once you use cloud storage or backup services. By shifting data from your internal storage space to someone else's you are usually required to analyze strongly exactly how that data will likely be stored so that you also may remain compliant with laws and industry rules [20][19].

Security Issues in Cloud Environment

Security issues in Deployment Models

Public Cloud- Public Clouds are experienced by way of regularly hacking effort.

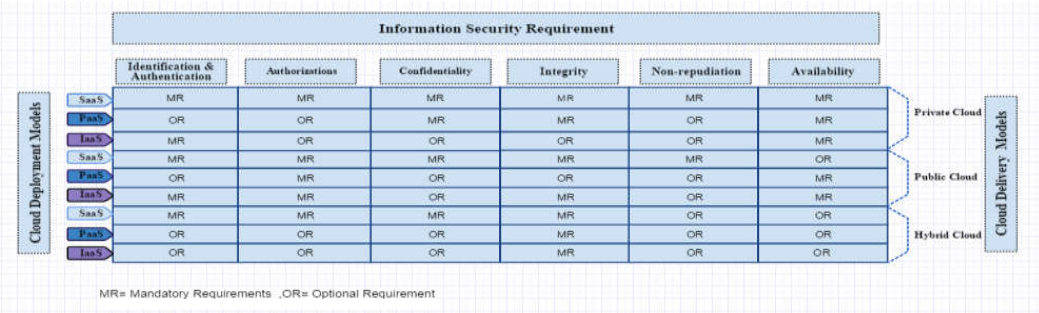


Figure 2 Security Requirements

There could possibly be more efficient way of authenticating the user such as x .509 certificates, one-time pass codes, and system fingerprinting.

Availability

The aim of availability for Cloud Processing systems that also includes applications and its own infrastructures is always to make sure its users can use them at anytime from anywhere.

Integrity

Once the data of a massage/an email is changed after the sender transmits it, but before it actually reaches to the expected recipient, after that the integrity of a massage/an email is lost.

Public Cloud providers are bigger targets for hackers as compared to private Clouds. Private Clouds has to be safe; there are still few significant attributes/properties of public Clouds to evaluate. Public Clouds equally draw the best security people offered, the most important and better Cloud service providers include a lot of customers depending on them[18][17]. They absolutely would be precise about who they use. Here is a list of a few other security issues regarding Public Cloud Computing:

Assessment of the cloud service provider

Most of the organizations are using the cloud computing for performance, cost and scalability. But the cloud also has risks. Therefore cloud service providers should have industry required certifications like the SAS70 Type II which is a physical examination that gives unbiased 3rd party confirmation, a service organization's insurance policies and types of procedures are properly developed.

Security of the communication channels

Data and communication security acts as an essential task in Cloud. Services are generally utilized via a thin client, laptop or mobile phone. The factors that your trusty data is quite easy to access by using most of these channels are your data is transmitted across several networks, further especially when your CSP is really isolated from where you are.

Transparency of security processes

Cloud Service Vendors are probably not going to make clear their security and safety approaches for their own particular security points. Because transparent relating to the controls they normally use to secure user data in the cloud.

Compliance with Regulations

PCIDSS, HIPAA, Geographical boundaries - The specific location of the data is substantial. To safe defend server failure Public Cloud service vendors will generally apply powerful data replication strategies. Which means the customer's data are circulated all over the world in different geographies.

Data Loss :Cross-tenant data

Leakage Weak points of shared network infrastructure factors, similar to weak points in a DNS server, Dynamic Host Configuration Agreement and IP protocol weak points, is possibly allowed network-based cross-tenant affects in an IaaS infrastructure.

Private Cloud- It contain the similar security issues as public Clouds. But, there exist some specific security problems regarding this Private Cloud model. The data security organization explained the new security problems of private cloud. The following are some ideas on providing a few security modifications in private cloud. They really are beyond the issues of scalability and accessibility, patch and configuration management must be seen, The stability and security of hypervisor need also be considered, In cloud management system, the lots of automation is also to be correctly protected and Stringent control really should be instead of Hypervisors to ensure security.

Security Control

Private cloud is usually available by one organization that offers the ability to configure and handle it based on their requirements to obtain a customized network option. The private cloud control structure should really allow handling to see security facets and indicate the existing risk phases of the environment. The manage direction is usually to be offered via an internet based control panel that converts the security problems into easy languages.

Compliance

Organizations like physical health and financial procedures belong to the auspices selection of contract needs and restrictions. With international organization it can also be potential those going to private cloud various list of restrictions are followed by several locations to gain access to data.

Security issues in service models

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

SaaS offer application services on demand such as conferencing application, e-mail and business applications like Customer Relationship Management (CRM), Enterprise resource planning (ERP), and Supply Chain Management (SCM). SaaS consumers have low control over security as compare to other service models. The adoption of SaaS applications can increase a few security issues.

Application security

Application security includes actions used during the code's life-cycle to reduce gaps in the security plan of an application via weak points in the deployment, update, or routine maintenance of the application. All these applications access by the internet. Attackers are going to use the internet to negotiate user's computers and execute harmful actions. Thus new strategies are needed because of traditional security solution does not provide protection from hacks.

Multi-tenancy

It is design for a single point of a software application serves many users. Each user is called a renter. Renters also have power to modify certain parts of the application. SaaS applications are arranged into maturity models which are based on scalability, configurability via metadata, and multi-tenancy.

Data security and Backup issue

Data security also grows a critical problem once SaaS customers depend upon their suppliers for proper security. In SaaS, organizational data files are normally organized in plaintext and saved in the cloud. The SaaS service provider is just one particular liable for the security of the data files when is required to be prepared and saved. Moreover, data back-up means that you can facilitate restore at the time of disaster, but it really introduces security problems as well. The SaaS provider wants to grantee that the using of encryption strategies to protect the backup data is advised to reduce accidental loss of sensitive data[1] [15].

Accessibility

Using applications by the internet can make access from any type of network device faster and easier, that includes public computing devices and cellphones. But, this also clarifies the services to other security problems. The Cloud Security Alliance is introducing an article that clarifies the present situation of mobile computing and also the leading threats in this field like unstable networks, vulnerabilities located in the device OS and standard applications, unsafe markets, and proximity-based hacking.

Platform-as-a-service (PaaS) security issues

PaaS provides deployment of cloud-based applications without the investment of purchasing and managing the necessary hardware and software layers. PaaS is based on a protected and trusted system and protected internet browser. PaaS application security and safety provides two software layers: Security of the PaaS setup itself and Security of user applications used on a PaaS platform. Similar to SaaS, PaaS also creates data security problems or other issues which are identified as follows:

Third-party relationships

PaaS offer common programming languages and also provide third-party web services components like mashups, which is merge multiple source component into a single integrated unit. Therefore, PaaS models also inherit security problems associated with mashups also PaaS customers must, depend upon both of them the security of web-hosted development tools and third-party solutions.

Resource Pooling and Rapid Elasticity issue

Various kinds of hardware and software assets are integrated for valuable use in cloud areas. This heterogeneity leads to defects as security configurations varies for different types of assets. Information leak is one issue due to shared assets.

Development Life Cycle

In development process, developers deal with the complexity of creating secure and safe applications which may be hosted and created in the cloud. The performance where applications will vary in the cloud will impact both the System Development Life Cycle (SDLC) and security. Developers must understand that PaaS applications needs to be updated regularly, so they really need to make sure their application development techniques are adjustable enough to get caught up with modifications.

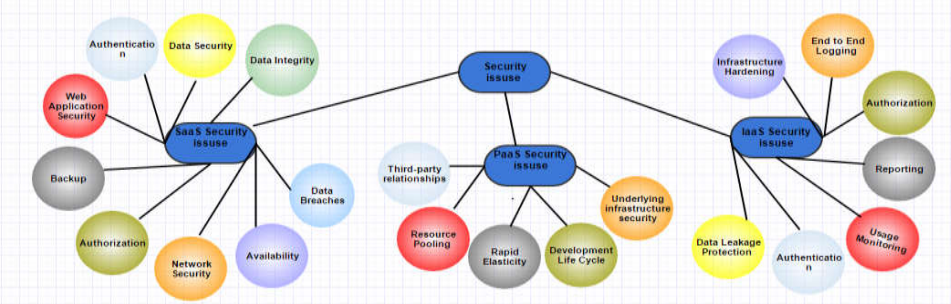


Figure: Security Issuse in Service Models

Underlying infrastructure security

Developers do not need use of the fundamental layers, so vendors are completely responsible for protecting the fundamental infrastructure and also the applications services. Even if developers are usually in control over the security of their applications, they just do not have the guarantee that the development environment tools offered by a PaaS supplier are safe.

Infrastructure-as-a-service (IaaS) security issues

It includes a group of assets like servers, warehouse, networks and other computing assets, which can be utilized by the Internet. With IaaS, cloud consumers have power over the security compared with the various other models as long it does not have any security hole in the virtual machine monitor. It vendors more attempt a major energy to protected their systems in an effort to reduce these threats that originate from creation, conversation, customization, and ability to move. A few security issues related to IaaS.

Data Leakage Protection and Usage Monitoring

Data saved in IaaS system on both private and public cloud has to be checked closely. It is important if IaaS is placed in public cloud. On this, it must be identified that who is actually using from where and what happened to used details later. It is usually fixed by making use of modern Rights Management services implementing limitation to business data. Policies for details must be prepared.

End to End Logging and Reporting

The successful deployment of IaaS needs basic logging and tracking in place. Secure logging and tracking solutions will keep track of where the details are, who accesses it, which devices are managing it and which storage arrays are completely responsible for it. These types of solutions are crucial for service management.

Authentication and Authorization

It can help to find helpful Data Loss Prevention solution. For each and every application, customer name and password is not best safe authentication system. At some time two factor or multi-factor authentication is required. We must consider demanding access policies depending on quality trust.

Infrastructure Hardening

"Golden-image" VM and VM concepts want to be hardened and cleaned up. This can be achieved while images are produced. On daily basis, testing associated with these master images must be done.

Computing Security Risk and Challenges

Isolation failure

Common resources and Multi-tenancy are features of cloud computing. From this group we examine the failure of process dividing the use of storage, routing, as well as status between various tenants.

Privileged user access

Data procedure out of organization is really harmful work, due to the fact that outside services avoid the physical, logical and

personal control. So handle the application, user want managerial control upon the application. In cloud deployments, clients generally provide control to the cloud provider over several issues which may have effect on security.

Regulatory compliance and Data protection

User wants security of their data in back and front both the end. Cloud service provider refuses this principle it give the features to utilize their application, services and responsibility of the cloud user to verify that the cloud provider provides justifiable certifications or not. Data security deals with several risk associated with data integrity, stealing, location, or loss. The avoidance of critical data is more useful, it also concerns damage or unavailability of data. Often, it can be hard for the cloud user to successfully verify the data proceeding services of the cloud provider and thus to be sure that the data is managed in a safe and sound way.

Vendor lock-in

The user require independence to shift their application and data from one provider to another, except that these may services do not help portability of applications and data to various other vendors that improve the threat of data and service unavailability. Thus users are successfully avoided from modifying and integrating to different vendors.

Management interface vulnerability

User control interfaces of a public cloud provider are likely to be available via the internet and mediate use of larger sets of resources compared to traditional providers. So this condition improved threat, when we merged remote access and web browser vulnerabilities.

Service unavailability

This is a result of some factors, from software Application or devices failures in the vender's data center, from problem of the communications between the user systems and provider services.

Solution of Security Issues

Cloud security architecture is very beneficial only after we apply specified rules to depending their architecture. We properly examine cloud security problems, challenges and risk.

Table 2 Issues and Solutions Summary for IAAS, PAAS, SAAS

Software-as-a-service (SaaS)	
Security Issues	**Possible solutions**
Authentication and Authorization	Two Factor Authentication , Open and clear Authorization , OAuth
Virtual Machine Security	Study on Virtual machine Security and safety, Reconfigurable distributed virtual machine , Secure VM by simply monitoring kernel and middleware stability.
Information Security	Information and facts Security Risk Management Framework
Cloud standards	Cloud Security Alliance (CSA) , Group ITU Cloud Computing Focus Group, IEEE Cloud Computing Standard Study
Data Access	Data Access Management ,Multi-user access policies
Web application security	Web Application Scanners
Backup	Agentless Method for data Backup and Recovery
Network Security	Network Security for virtual machines, Network Security Sandbox.
Data confidentiality	Characteristic based Proxy Re-Encryption
Availability	Data Dispersion
Identity management and sign-on process	CSA's Identity and Access Management Guidance
Platform-as-a-service (PaaS)	
Security Issues	**Possible Solutions**
Interoperability	Trusted Computing Base
Object Vulnerability	Encryption
Privacy Aware Authentication	Proxy Certificates
Host Vulnerability	Trusted Computing Base
Access Control	Policy Enforcement Points, Undeniable Logging Protocol, Encapsulation
Service Continuity and Fault Tolerance	Byzantine Quorum System
Infrastructure-as-a-service (IaaS)	
Security Issues	**Possible Solutions**
Monitor QoS attributes	SLA monitoring and enforcement in SOA
Monitoring and enforcing SLA.	Web Service Level Agreement (WSLA) framework.
Determining and billing with Several stages of providers On-demand billing system availability.	Amazon DevPay.
Attacks against XML, Attacks against web services.	XML Signature and XML Encryption, SOAP Security Extensions.
DDOS, Man-In-The-Middle attack (MITM), IP Spoofing, Port Scanning, DNS security.	Logical Network segmentation and Firewalls, Traffic encryption, Network monitoring, Intrusion Detection System and Intrusion Prevention System (IPS).
Security threats sourced from host: • Observing VMs from host. • VMs modification. • Conversations between VMs and host.	Security threats sourced from host: • Trusted Cloud Computing Platform • Mandatory Access Control MAC • Trusted Virtual Datacenter (TVDc)
Data security on not open or modified storage devices. Actual physical attacks against computer machine	Higher secure locked rooms with monitoring appliances. Multi-parties gain access to encrypted storage. Clear cryptographic file systems. Self-encrypting enterprise tape drive TS1120.
Security threats acquired from VM: • Virtual machines Mobility • Resources Denial of Service. • Monitoring VMs from other VM. • VMs provisioning and migration. •Communication between VMs.	Security threats acquired from VM: • Virtual Private Network (VPN). • Xen Security through Disaggregation. • IPSec. • LoBot architecture for secure provisioning & migration VM • Encryption.

For each and every worms and risk, we determine which cloud service model or models respond to these types of security issues. There is several easy manner or technique, that help to secure and protected cloud [21][23].

Identity and access management guidance

Cloud Security Relationship is a non-profit organization which offers the utilizing most effective techniques to provide security in cloud situations. It includes issued a verification and Have access to Management Guidance that offers a listing of suggested best practiced to ensure identities and secure and safe access control.

Use of Encryption Technique and Digital signatures

Encryption methods are used form a long time to protected very sensitive data. Always make sure that data is protected once that is encrypted in time of Shifting or putting in the cloud. Also Digital signature is a method use to check authentication and reliability of data and software program. A lot of researcher give advice to protected data using digital signature with RSA algorithm during data is being moved via the internet.

Virtual network security

A virtual network framework to protect the conversation between virtual machines. This framework designed two configuration models for virtual networks. The majority of virtual network designs are contains three layers: firewall, shared networks and routing layers that may reduce VMs from sniffing and spoofing [5] [6].

Proper understanding of SLAs (Service Level Agreements)

Service level agreement provides arrangement between the vendor and user in term of range, quality and responsibilities. Based on the SLA every provider and user having a lot of job that is needed to decide on protected cloud because amount of performance observed both sides regularly [1].

Recovery Facilities

Cloud providers should try to give helpful recovery advantages. Therefore details are fragmented or lost due to some kind of harm, they can easily be restored and continuity of information and data may be managed also [9].

Use of Better Enterprise Infrastructure

Organization give infrastructure that enables unit installation and plan of hardware choices like routers, servers, proxy servers , firewalls ,software like operating system and so many. Most of us need an infrastructure that minimizes harmful process and affects.

ANALYSIS AND DISCUSSION

SaaS includes issued an Identification and Gain access to Control Guidelines to provide a summary of really helpful ideal practices to ensure identities and safe gain access to control. Applications are deployed in PaaS without requiring purchasing and maintaining the hardware components store and software there by based on a secure browser. PaaS application security includes the security of application deployed on PaaS and also the PaaS platform security itself[7] [11] [16].

Additionally this implies the relationship between IaaS elements and protection requirements, and facilitates security advance in specific levels to get an entire protect IaaS structure [9][10]. Table shows the overview of security issues with their solutions in cloud service models [8] [13] [22].

CONCLUSION

In recent years cloud computing is an upgraded concept that gives profits for the users. But, this also increases a few security issues, which sometimes go slower its development. Knowledge about vulnerabilities in the cloud should help organizations shift in the direction of the Cloud. In this article we have included a fundamental description of cloud computing as well as reviewed the security and safety issues/concerns associated with cloud development and service models. In terms of security issues private cloud provides the maximum report. Security problems for cloud service models are differ based on the model. That is why, security will almost always be a problem. This paper also gives information about the security risk and difficulties which kept the growth of cloud computing.

Here we distinctly study, security issue with cloud models and challenges related to provisioning end user in cloud computing. Additionally, we presented some solutions that may really help to maintain secure and safe cloud.

References

1. Security for Cloud Computing by Cloud Standards Customer Council, 2012.
2. Tamanna Siddiqui, and R. Ahmad. “Cloud Testing–A Systematic Review.” *International Research Journal of Engineering and Technology* (IRJET) Volume: 02 Issue: 03, June-2015.
3. Mell P and Grance, “The NIST definition of Cloud Computing”. Gaithersburg, MD: NIST, Special Publication 800–145, 2011.
4. Pradeep Kumar Tiwari and Bharat Mishra,“ Cloud Computing Security Issues, Challenges and Solution”, *International Journal of Emerging Technology and Advanced Engineering*, ISSN 2250-2459, Volume 2, Issue 8, August 2012.
5. S. Sharma, G. Gupta and Laxmi, “A survey on cloud security issues and techniques”, 2014.
6. P.K.Tiwari and B.Mishra, “Cloud Computing Security Issues, Challenges and Solution.” *International Journal of Emerging Technology and Advanced Engineering*, ISSN 2250-2459, Volume 2, Issue 8, August 2012.
7. B.Angadi, Abhinay, Akshata B. Angadi, and Karuna C. Gull. "Security Issues with Possible Solutions in Cloud Computing-A Survey." *International Journal of Advanced Research in Computer Engineering & Technology* (IJARCET) Volume 2, Issue 2, pp-652, February 2013.
8. Bisong and Rahman, “An overview of the security concerns in enterprise cloud computing”, *International Journal of Network Security & Its Applications* (IJNSA), Vol.3, No.1, January 2011.
9. Rai, Rashmi, G. Sahoo, and S. Mehfuz. “Securing software as a service model of cloud computing:

Issues and solutions." *International Journal on Cloud Computing: Services and Architecture* (IJCCSA), Vol.3, No.4, August 2013.

10. W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions." In Informatics and Systems (INFOS), the 7th International Conference on (pp. 1-8). IEEE, March 2010.
11. T.Devi, and R. Ganesan. "Platform-as-a-Service (PaaS): Model and Security Issues." TELKOMNIKA *Indonesian Journal of Electrical Engineering*, Vol. 15, No. 1, pp. 151-161 , July 2015.
12. NIST Definition of Cloud Computing v15, csrc.nist.gov/groups/ SNS/cloud-computing/cloud-def-v15.doc.
13. Chavan, Pragati, *et al*. "IaaS Cloud Security." Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on. IEEE, 2013.
14. Shushing Yu, Cong Wang, Kui Ren, and Wenjing Lou. "Achieving secure, scalable and fine-grained data access control in cloud computing", in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.
15. Krutz, L. Ronald and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 179-80, 2010.
16. Y. Chen, V. Paxson, and R. Katz, "What's New about Cloud Computing Security?" 2010.
17. Kuyoro S. O., Ibikunle F. & Awodele O "Cloud computing security issues and challenges." *International Journal of Computer Networks (IJCN), Volume* (3), Issue (5), 2011.
18. Chen, Yanpei, Vern Paxson, and Randy H. Katz. "What's new about cloud computing security?" University of California, Berkeley Report No. UCB/EECS-2010-5 January 20.2010.
19. Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and Atanu Rakshit. "Cloud security issues." Services Computing, 2009. SCC'09. IEEE International Conference on. IEEE, 2009. V
20. Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. "The management of security in cloud computing." Information Security for South Africa (ISSA), IEEE, 2010.
21. Songjie, Junfeng Yao and Chengpeng Wu, "Cloud computing and its key techniques".
22. Bernsmed, Karin, *et al*. "Security SLAs for federated cloud services." Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. IEEE, 2011.
23. Rao, R. Velumadhava, and K. Selvamani. "Data Security Challenges and Its Solutions in Cloud Computing." Procedia Computer Science pp. 204-209, 2015.
24. Rong, Chunming, Son T. Nguyen, and Martin Gilje Jaatun. "Beyond lightning: A survey on security challenges in cloud computing." Computers & Electrical Engineering, pp. 47-54, 2013.
25. Dr. Tamanna Siddiqui, Mohammad Al Kadri ; Big Data Analytics on the Cloud; *International Journal of Emerging Technologies in Computational and Applied Sciences* (IJETCAS); IJETCAS 15-752; © 2015, page No, 61-66; ISSN (Online): 2279-0055.

****

How to cite this article:

Najeeb Ahmad Khan., Tamanna Siddiqui and Riaz Ahmad.2016, Review On Cloud Security Issues: Challenges And Solutions. *Int J Recent Sci Res.* 7(5), pp. 10846-10853.

TSSN 0976-3031