International Journal of Management, IT & Engineering
Vol. 8 Issue 10, October 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

VULNERABILITY ISSUES AND CHALLENGES IN NEW ERA OF SPINC MODEL

TeenaJaiswal*

R N Jaiswal**

Chanchala Joshi***

Abstract

Cloud computing is a model for delivering data technology services within which resources area unit retrieved from the net through web-based tools and applications instead of an instantaneous association to a server .Contrarily to traditional on site application design wherever applications are residing in consumer machines or in a very server accessible via client cloud computing offers shared pc application resources and accessible via the net. Since cloud computing share distributed resources via the network within the open setting, it presents an additional level of risk as a result of essential services are usually outsourced to a third party, that makes it tougher to take care of information security and privacy, support information and repair available, and demonstrate compliance. Numerous classes of such security considerations are trust, design, identity management, package isolation, information protection, confidentiality and available. All these security vulnerabilities cause many threats on the cloud like authentication, misuse of cloud infrastructure, eavesdropping, network intrusion, DOS attack, session hijacking. Cloud Computing represents the Internet-based

Keywords:

Cloud Computing Services;

Virtual Private Cloud;

Distributed Computing;

Vulnerability ;

SPINC Model.

***Department of Computer Science, MakhanlalChaturvedi National University. BHOPAL (M.P) India**

****Department of Computer Science, Rashtriya Military School Shimla (H.P) India**

*****Institute of Computer Science Vikram University, Ujjain, M.P.India**

platform for computing. It is the services offered via the web. its actual shopping for of services from the service supplier, But because the data is unbroken at the third-party location, these results in plenty of insecurities within the minds of service owner. Hence, it results in plenty of security considerations. This research paper analysis to SPINC service and deployment mode l. it conjointly inherits their security problems, that we tend to discuss here, distinguishing the most vulnerability during this reasonably system and (omit) the most vital threats found within the literature associated with Cloud.

1. Introduction

Cloud computing could be a new paradigm that permits scalable services to be wiped out over the net .Users knowledge is largely processed on a distant machine. it's primarily a service on demand, that is, the service is provided once it's demanded by the user. it's primarily has 5 options that makes it a distinction from alternative rising trend – multitenancy , elasticity , quantifiability , pay per usage and self-provision of resources . Multi-tenancy relies on the very fact that the resources are often shared. Scalability is ability to scale to thousands of system. Physical property refers to extend or decrease of the computing resources as per the user's requirement. Pay per use model refers to the very fact that we want to pay just for that we tend to use. The cloud computing model defined has six essential service model and five deployment model. Six service model also called SPINC model ,are : Software as Service (SaaS), Platform as a Service (PaaS) , Infrastructure as a Service (IaaS), Network as a Service(NAAS)[1], Communication as a Service(CAAS)[2] and Security as a Services (SecAAS)[3].

The five deployment Models are: Private cloud, Public cloud and Hybrid cloud, Community cloud[4], Network cloud[5].

There is two table shown below which represent cloud computing and deployment model in details.

Table 1.Cloud computing service model are explain in below

Service Model	Description	Characteristics	Disadvantages & Risks	Provider
SAAS	a complete application is offered to the customer, as a service on demand	SLAs; UI powered by "thin client" applications; cloud components; communication via APIs; stateless; loosely coupled; modular; semantic interoperability	Centralization of data requires new/ different security measures	Google, Salesforce, Microsoft, Zoho
PAAS	a layer of software system, or development setting is encapsulated & offered as a service, upon that alternative higher levels of service may be engineered.	Consumes cloud infrastructure; caters to agile project management methods	Centralization requires new/ different security measures	Azure ,LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google"s App Engine, Force.com
IAAS	Provides basic storage and computing capabilities as standardized services over the network.	Usually platform independent; infrastructure costs are shared and thus reduced; service level agreements (SLAs); pay by usage; self-scaling	Business efficiency and productivity largely depends on the vendor's capabilities; potentially greater long-term cost; centralization requires new/ different security measures	Amazon, GoGrid, 3 Tera
CAAS	It provides Software as a Service (SaaS) for communications.	Voice mail feature, customer care, security, audio and video conferencing.	quality and the reliability of these solutions is of primary concern. critical nature of telephony.	Facebook, Whatsapp,InternetMessanger

NAAS	Network and transport connectivity is provided as a service by cloud provider.	Optimal flexibility in capacity control, Optimal network activity and/or bandwidth utilisation within minimal downtime, Improved network efficiency, Fast deployment	storage, processing and delivery closer to the network edge mean service reliability and quality is increased overall and local network problems are less likely to have global side-effects.	Cisco (CSCO), IBM (IBM), VMware (VMW), and Juniper (JNPR)
SeAAS	Delivers managed security services over the internet.[6]	Data loss prevention ,web security, intrusion management ,network security	Loss or theft of intellectual property, Malware infections that unleash a targeted attack, Revenue losses, Loss of control over end user actions	Cisco, McAfee, Panda Software, Symantec, Trend Micro and VeriSign. Qualys

Table 2 Cloud Computing Deployment models

Deployment model	Description	Security	Service provider
Private cloud	Private clouds provide services to the customers of the particular organizations for the sake of security and confidentiality of their personal data. The fact is that whether these private clouds are owned and controlled by customers but they are built and installed by the third parties.	i)Least secure ii)Multitenancy iii)Transfers over the net	VMware ,Microsoft , Amazon EC2 Eucalyptus
Public cloud	Public clouds are not restricted to any particular customers or organizations. They provide services to the	i)Least secure ii) Multitenancy iii)Transfers over the net	Amazon Elastic , Google App Engine, Blue Cloud by IBM and ,Azure

	public all over the world without any limitations. But they are not as secure as private clouds.		services Platform by Windows
Hybrid cloud	Hybrid clouds are the combination of both public and private clouds. The organizations and other people can take benefits of both public and private cloud by using hybrid clouds. Like some of the companies set their own private clouds and they take services from it but if they need some services from public cloud also then this facility comes under hybrid clouds only.	Control of security between Private and Public clouds	CTERA , Red hat open hybrid cloud
Community cloud	The cloud infrastructure is shared between the organizations with similar interests and requirements whether managed internally or by a third-party and hosted internally or externally.	Fixed amount of bandwidth and data storage is shared among all community members.	all the government agencies in a city can share the same cloud but not the non-government agencies
Network cloud	Networking resources from a centralized third-party provider using Wide Area Networking (WAN) or Internet-based access technologies.	Account hijacking, Malicious insiders ,Data breaches	IBM, Zhou

2.SECURITY ISSUES OF CLOUD COMPUTING

Cloud Computing controls several existing technologies like net services, net browsers, and virtualization, that contributes to the evolution of cloud environments. Therefore, any vulnerability associated to those technologies in addition affects the cloud, and it'll even have a giant impact. Speedy cloud adoption has but, introduced distinctive and sophisticated security considerations for users. Presently organizations ought to take under consideration however adopting a cloud-computing model will have a sway on their risk profile related to information security, privacy and convenience. Complicating that assessment is that the undeniable fact that presently among the last word security of cloud implementations is Associate in Nursing inherent partnership with the cloud service provider. Aspects like physical security, configuration integrity and personnel vetting is presently inside the hands of the provider, that the majority organizations taking advantage of the cloud never see.[8] From varied Associate in Nursing analysis articles can we'll (we area unit going to) conclude that information storage and virtualization are the foremost essential degree an attack to them will do the foremost injury. Attacks to lower layers have additional impact to the alternative layers. We tend to tend to position plenty of stress on threats that area unit associated with information being hold on and processed remotely, sharing resources and conjointly the usage of virtualization. for each vulnerability and threat, we tend to determine what cloud service model or models area unit plagued by these security problems. This analysis counsel fast description of the vulnerabilities, and specifies what cloud service models (S-SAAS,P-PAAS,I-IAAS,N-NAAS,C-CAAS) area unit usually plagued by them. For this analysis, we tend to tend to focus within the main on technology-based vulnerabilities.

3.Vulnerabilities Issues in VPC

The increasingly frequent use of VPC created new security risks. Thereby increasing the interest of hackers to seek out new vulnerabilities and exposing users to examine their data compromised .Vulnerability should be portrayed in terms of resistance to a particular reasonably attack. to produce a real-world example, a car’s inability to safeguard its driver against injury once hit frontally by a truck driving sixty mph might be vulnerability; the resistance of the car’s crumple zone is only too weak compared to the truck’s force. Against the “attack” of a biker, or maybe a bit automobile driving at a further moderate speed, the car’s resistance strength is totally adequate.

3.1.Data Breaches

A information breach might lead to data loss, as well as monetary, personal and health data. A hacker conjointly might use taken information to impersonate himself to realize access to a safer location. for instance, a hacker's information breach of a network administrator's login credentials may end up in access of a whole network. The cloud comes with a singular set of characteristics that create it a lot of vulnerable.[9]

3.2. Hijacking of Accounts

The growth and implementation of the cloud in many organizations has opened a full new set of issues in account hijacking. Attackers presently have the ability to use your (or your employees') login information to remotely access sensitive information continue the cloud; else, attackers can falsify and manipulate information through hijacked credentials. alternative ways that of hijacking embrace scripting bugs and reused passwords, which enable attackers to easily and sometimes whereas not detection steal credentials. In New Style calendar month 2010 Amazon round-faced a cross-site scripting bug that targeted consumer credentials additionally. Phishing, key work, and buffer overflow all gift similar threats. However, the foremost notable new threat – referred to as the person In Cloud Attack – involves the thieving of user tokens that cloud platforms use to verify individual devices whereas not requiring logins throughout each update and regulate.[10]

3.3. Insider Threat

An corporate executive attack within the cloud is less complicated to perform and has way bigger impact than Associate in Nursing attack in a very ancient infrastructure. At an equivalent time, detection and identification of the physical entity that performed the attack remains difficult.[11] an corporate executive threat was the misuse of knowledge through malicious intent, accidents or malware.

3.4. Malware Injection

Malware injection attack is one class of web-based attacks, within which hackers exploit vulnerabilities of an online application and enter malicious codes into it that changes the course of its traditional execution. Like web-based applications, cloud systems also are prone to malware injection attacks. Hackers craft a malicious application, program, and virtual machine and inject them into target cloud service models SaaS, PaaS and IaaS, severally. Once the injection is completed, the malicious module is dead collectively of the

valid instances running in the cloud; then, the hacker will do no matter s/he wishes like eavesdropping, data manipulation, and knowledge stealing[13] .Malware injections area unit scripts or code embedded into cloud services that act as "valid instances" and run as SaaS to cloud servers. this suggests that malicious code are often injected into cloud services and viewed as a part of the software package or service that's running inside the cloud servers themselves. Once AN injection is dead and also the cloud begins operational in cycle with it, attackers will listen, compromise the integrity of sensitive info, and steal knowledge [12].

3.5. Abuse of Cloud Services

The growth of cloud-based services has created it doable for each tiny and enterprise-level organizations to host huge amounts of knowledge simply. However, the cloud's new storage capability has conjointly allowed each hackers and approved users to simply host and unfold malware, contraband computer code, and alternative digital properties. In some cases this apply affects each the cloud service supplier and its shopper. for instance, privileged users will directly or indirectly increase the safety risks and as a result infringe upon the terms of use provided by the service supplier [14].

3.6.Insecure APIs

Application Programming Interfaces (API) provides users the chance to modify their cloud expertise. However, APIs are often a threat to cloud security thanks to their terrible nature. Not solely do they provide corporations the power to customize options for their cloud services to suit business desires, however, they conjointly manifest, offer access, and impact secret writing. As the infrastructure of APIs grows to supply higher service, therefore do its security risks. APIs provide programmers with the tools to make their programs to integrate their applications with an alternative job-critical software package. a well-liked and easy example of associate degree API is YouTube, wherever developers have the power to integrate YouTube videos into their sites or applications. The vulnerability of associate degree, API lies within the communication that takes place between applications. Whereas this could facilitate programmers and businesses, they conjointly leave exploitable security risks [15].

3.7. CSRF Attacks

Cross-Site Request Forgery (CSRF) may be a ton like XSS.The distinction between the two is that CSRF exposes vulnerabilities on the server facet, not the consumer facet. A CSRF attack tricks the server into process auserrequest that has been sent by an unauthorized user. By including a legitimate session id within the HTTP request, the server would suppose that the request is real and proceed with the method. merely removing the session id from the url and setting it as a cookie doesn't forestall CSRF. The only technique that works is that the inclusion of a random token with each request, one that may not be guessed by an attacker. This token will then give authentication thatthe request has been sent from the authorized user [16].

3.8. Denial of Service Attacks

Unlike different reasonably cyber-attacks, that square measure generally launched to ascertain a semi-permanent foothold and hijack sensitive data, denial of service assaults don't decide to breach your security perimeter. Rather, they decide to create your web site and servers unavailable to legitimate users. In some cases, however, DoS is additionally used as a smokescreen for different malicious activities, and to require down security appliances like net application firewalls [17].

3.9. Insufficient Due Diligence

With cloud computing being a replacement implementation, particularly to the hiring organisations, there's a data gap that may forestall ample exercise of due diligence once hiring a cloud service supplier. while not knowing quite what they're catching for, customers will realize a match between what they assume they're obtaining and what a CSP will give. Asking the correct queries is important, therefore, to understanding the written agreement obligations and liabilities of supplier and client. Service agreements would possibly fail to debate revelation within the face of an occurrence. Enterprise architects may not ensure whether or not their on premise security controls are going to be effective within the cloud .Hiring organizations conjointly should ensure to decide on a cloud supplier which will not arrange to lock them in if the service ought to prove unacceptable, or if the organisation desires to use services from another supplier. If the connection has to be terminated, the recent CSP should be willing and able to go on and delete the organisation’s knowledge firmly and expeditiously.

3.10. Shared Vulnerabilities

Cloud security could be a shared responsibility between the supplier and also the consumer. This partnership between consumer and supplier needs the consumer to require preventative actions to guard their information. whereas major suppliers like Box, Dropbox, Microsoft, and Google do have standardized procedures to secure their aspect, fine grain management is up to you, the client. Cloud computing by its definition – that of shared infrastructure – depends on the cooperation of multiple devices during a virtual setting, associate degreed in such an design, the infiltration and management of only 1 of these devices – particularly the hyper visor – exposes all customers to a breach UN agency square measure tenants in this setting. this is often additionally true for different shared services offered by the supplier, together with shared applications, shared operational systems, shared Apis, and shared storage [19].

3.11. Data Loss

Data on cloud services are usually lost through a natural disaster, malicious attack, or a data wipe by the service provider. Losing vital information is usually devastating to businesses that don't have a recovery started. Amazon is an associate example of a company that suffered data loss by permanently destroying many of its own customers' data in 2016. Google was another organization that lost data once its facility was full of lightning fourfold. Securing your data suggests that strictly reviewing your provider create a replica procedure as they relate to physical storage locations, physical access, and physical disasters [20].

4. Challenges in Cloud Communication Model

The communication method leads to transmission of either data/information or applications between the Customer and therefore the cloud. Moreover, there exists communication at intervals cloud between VMs.

4.1. Virtual Private Network

In cloud computing systems, the communication takes place not solely on real networks however virtualized networks conjointly play a vital role in communication.

4.1.1 Virtual network

virtual networks could be a logical network engineered over a physical network. The virtual networks square measure to blame for communication between VMs. The software-based network parts, like bridges, routers, and software-based network configurations,

support the networking of VMs over a similar host. The virtualized networks square measure able to generate the subsequent security challenges within the cloud atmosphere. Security and protection mechanisms over the physical network aren't able to monitor the traffic over the virtualized network. This becomes a significant challenge as malicious activities of the VMs transcend the observation of security tools. Intrusion sighting and hindrance mechanisms sometimes depend upon the traffic patterns and activities to gauge the anomalies and detect the likelihood of the attack. Virtualized network poses a hindrance to the goal of such preventive measures [7]. The virtualized network is shared among multiple VMs that cause the likelihood of bound attacks, such as, Denial of Service (DoS), spoofing and sniffing of the virtual network. The traffic rates are often monitored for malicious functions. The cryptanalytic keys become prone to escape, just in case of malicious sniffing and spoofing of the virtual network [11]. the information in transit happiness to users will suffer from pricey breaches.

4.1.2. Virtualization

Virtualization permits users to make copy, share, migrate, and roll back virtual machines, which can enable them to run a spread of applications. However, it additionally introduces new opportunities for attackers thanks to the extra layer that has got to be secured . Virtual machine security becomes as vital as physical machine security, and any flaw in either one could have an effect on the opposite [18]. Virtualized environments area unit prone to all types of attacks for traditional infrastructures; but, security may be a bigger challenge as virtualization adds additional points of entry and additional interconnection quality not like physical servers, VMs have 2 boundaries: physical and virtual [21].

5. Issues of Virtualization

Virtualization is one in every of the strategic elements of the cloud. Virtualization permits the utilization of same physical resources by multiple customers. A separate VM is instantiated for every user that nearly provides a whole in operation machine to the user . many VMs are often mapped to constant physical resources permitting the resource pooling in multi-tenant surroundings. A VM monitor (VMM) or hyper visor is that the module that manages the VMs and permits varied in operation systems to run at the same time on constant physical system. not with standing, virtualization conjointly introduces security challenges to the cloud users and infrastructure [22]. we tend to discuss the safety problems associated with virtualization below.

5.1 VM image sharing

A VM image is employed to instantiate VMs. A user will produce his/her own VM image or can use a picture from the shared image repository. The users area unit allowed to transfer and transfer pictures from the repository (for example Amazons image repository) Sharing of VM pictures within the image repositories could be a common apply and might evolve as a significant threat if it's employed in malicious manner . A malicious user will investigate the code of the image to appear for probable attack purpose. On the opposite hand, a malicious user will upload a picture that contains a malware. The VM instantiated through the infected VM image can become source of introducing malware within the cloud system. Moreover, AN infected VM will be wont to monitor the activities and knowledge of alternative users leading to privacy breach. Likewise, if the image isn't properly cleaned, it will expose some counselling of the user [23].

5.2 VM Isolation

VMs running on identical physical hardware have to be compelled to be isolated from one another. Although logical isolation is gift between completely different VMS, the access to same physical resources will result in knowledge breach and cross-VM attacks. Isolation isn't solely required on storage devices however memory and machine hardware additionally wants fine grained isolation of VMs [24].

5.3 VM escape

VM escape may be a state of affairs within which a malicious user or VM escapes from he management of VMM or hypervisor. A VMM may be a package element that manages all the VMs and their access to the hardware. The VM escape state of affairs will give aggressor access to alternative VMs or will bring the VMM down . A flourishing VM escape attack will give access to the computing and storage hardware. The IaaS service model is affected which will successively result alternative service models [25].

5.4 VM migration

The VM migration is that the method of relocating a VM to a different physical machine while not shutting down the VM. The VM migration is meted out for variety of reasons, like load equalisation, fault tolerance, and maintenance. Throughout the migration section, the contents of the VM are exposed to the network which may result in knowledge privacy and integrity issues. Besides knowledge, the code of

VM additionally becomes at risk of attackers throughout migration. The migration modules are often compromised by Associate in Nursing aggressor to relocate the VM to a compromised server or below the management of compromised VMM. The VM migration may be a crucial section and desires to be meted out during a secured manner.[26].

5.5 VM rollback

Virtualization permits the rollback of a VM to some previous state whenever it's required. The rollback feature provides flexibility to the user. However, rollback conjointly raises security considerations. For example, the rollback will change the safety credentials that were antecedent disabled. Moreover, the rollback may render the VM to a vulnerability that was antecedent patched. what is more, the rollback will revert the VM to previous security policies and configuration errors[27].

5.6 Hypervisor issues

The key module of virtualization is hypervisor or VMM. The VMs management and isolation is that the responsibility of the VMM. Generating and managing virtual resources, is yet one more perform performed by the VMM. A VMM could have an effect on the execution of VMs running on the host system . A compromised VMM will place all the VMs that area unit managed by the victim VMM below attacker's management . The information of the VMs, unbroken by the VMM, may additionally be exposed to Associate in Nursing wrongdoer if the wrongdoer takes management of a VMM . A VMM will offer larger attack vector owing to a lot of entry points and interconnection complexities There area unit several reported bugs within the VMM that permit the wrongdoer to require management of the VMM or bypass security restrictions. as an example, vulnerabilities within the Xen, Microsoft Virtual laptop, and Microsoft Virtual Server may be abused by attackers to realize privileged rights [28].

5.7 VM sprawl

VM sprawl could be a scenario wherever variety of VMs on the host system is unceasingly increasing and most of the already instantiated VMs area unit in idle state. The VM sprawl causes the resources of the host machine to be wasted on giant scale.[29].

6. Conclusion

Cloud computing may be a promising and rising technology for successive generation of IT applications. Although cloud computing has several blessings, there square measure still several actual issues that require to be solved. The revenue estimation implies that cloud computing may be a promising trade. However from another perspective, existing Vulnerabilities within the cloud model can increase the threats from hackers. Per service delivery models, deployment models and essential options of the cloud computing, information security and privacy protection problems are the first issues that require to be solved as presently as attainable. Information security and privacy problems exist altogether Levels in SPINC service delivery models and altogether stages of knowledge life cycle. The challenges in privacy protection square measure sharing information whereas protective personal data. The everyday systems that need privacy protection square measure ecommerce systems that store credit cards and health care systems with health information. the flexibility to manage what information to reveal and World Health Organization will access that data over the net has become a growing concern. These considerations embrace whether or not personal data is keep or scan by third parties while not consent or whether third parties will track the net sites somebody has visited. Another concern is whether or not websites that are visited collect, store, and probably shares personal data concerning users. Reducing information storage and processing price may be a necessary demand of any organization, whereas analysis of knowledge and knowledge is always the foremost vital tasks altogether the organizations for deciding. Therefore no organizations can transfer their information or data to the cloud till the trust is made between the cloud service suppliers and shoppers. A number of techniques are projected by researchers for information protection and to achieve highest level of knowledge security within the cloud. However, there square measure still several gaps to be stuffed by creating these techniques more practical. More work is needed within the space of cloud computing to create it acceptable by the cloud service shoppers. This paper surveyed the key security problems with Cloud Computing being featured nowadays and also the challenges and opportunities that it brings for businessmen. This analysis paper analysed what precisely cloud computing security-related problems square measure, and mentioned information security and privacy protection problems related to cloud computing across all stages of knowledge life cycle.

Future work projected can facilitate identity management system to attain additional automatic and quick user account provisioning and de-provisioning so as to make sure no un-authorized access to organizations' cloud resources by some workers World Health Organization has left the organizations. Authorization and access management mechanisms can get to succeed a unified, reusable and climbable access control model and meet the necessity of fine-grained access authorization. answerability primarily based privacy protection mechanisms can succeed projectile and period of time inform, authorization and auditing for the information house owners once their non-public information being accessed.

References

[1] Duan, Qiang, Yuhong Yan, and Athanasios V. Vasilakos. "A survey on service-oriented network virtualization toward convergence of networking and cloud computing." IEEE Transactions on Network and Service Management 9.4 (2012).

[2] Subashini, Subashini, and VeerarunaKavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[3] Hussain, Mohammed, and HanadyAbdulsalam. "SECaaS: security as a service for cloud-based applications." Proceedings of the Second Kuwait Conference on e-Services and e-Systems.ACM, 2011.

[4] Goyal, Sumit. "Public vs private vs hybrid vs community-cloud computing: a critical review." International Journal of Computer Network and Information Security 6.3 (2014): 20.

[5] Lin, Yonghua, et al. "Wireless network cloud: Architecture and system requirements." IBM Journal of Research and Development 54.1 (2010): 4-1.

[6]Mohammed Hussain, HanadyAbdulsalam,SECaaS: "security as a service for cloud-based applications", ACM New York, NY, USA ©2011 .

[7] FarzadSabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", Int. Journal of Machine Learning and Computing, pp.39-45, vol. 2, no. 1, February, 2012.

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

[9] Ponemon Institute© Research Report, “Man In Cloud Attack” .

[10] Amazon purges account hijacking threat from site,2016

[11] Salem M., Hershkop S., Stolfo S.J., “A Survey of Insider Attack Detection Research”, Insider Attack and Cyber Security, Springer, 2008, Vol. 39, pp. 69-90, 2008.

[12] Web Based Attacks, Symantec White Paper, February 2009

[13] PriyankaChouhan, Rajendra Singh,” Security Attacks on Cloud Computing With Possible Solution”, IJARCSSE ,Volume 6, Issue1, January 2016

[14] The Notorious Nine Cloud Computing Top Threats in 2013

[15] Kumar Gunjan , R. K. Tiwari , G. Sahoo ,” Towards Securing APIs in Cloud Computing”, International Journal of Computer Engineering & Applications, Vol. II, Issue II,2013.

[16]Ding, Chaohai. "Cross-site request forgery attack and defence: literature search." (2013).

[17] Neha Gupta, RajetVeshin, Rajneesh Sharma,” Distributed Denial of Service (DDOS) Attacks in Cloud Computing: A Survey”, International Journal of Enhanced Research in Management & Computer Applications ISSN: 2319-7471, Vol. 4 Issue 12, December-2015.

[18] S. Venkata Krishna Kumar, S.Padmapriya,” A Survey on Cloud Computing Security Threats and Vulnerabilities”, INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING Vol. 2, Issue 1, January 2014.

[19] BijayalaxmiPurohit,PawanPrakash Singh,” Data leakage analysis on cloud computing”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 3, May-Jun 2013.

[20] Charles PEREZ, Babiga BIRREGAH, Marc LEMERCIER, “The Multi-layer imbrication for data leakage prevention from mobile devices” in IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,2012.

[21] Poonam V. Kapse, R. C. Dharmik, "An effective approach of creation of virtual machine in cloud computing", I-SMAC (IoT in Social Mobile Analytics and Cloud) (I-SMAC) 2017 .

[22] Durairaj. M, Kannan.P," A Study On Virtualization Techniques And Challenges In Cloud Computing", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 3, ISSUE 11, NOVEMBER 2014.

[23]Ivan Studnia, Eric Alata, Yves Deswarte, Mohamed Kaâniche, Vincent Nicomette. Survey of Security Problems in Cloud Computing Virtual Machines.Computer and Electronics Security Applications Rendez-vous (C ESAR 2012).

[24] Eddy Caron, Jonathan Rouzaud-Cornabas. Improving Users' Isolation in IaaS: Virtual Machine Placement with Security Constraints.7th IEEE International Conference on Cloud Computing (IEEE Cloud 2014), Jun 2014.

[25] Jiang Wu , *, Zhou Lei, Shengbo Chen and WenfengShen," An Access Control Model for Preventing Virtual Machine Escape Attack", MDPI, Basel, Switzerland, June 2017.

[26] Suresh B.Rathod, V.Krishna Reddy," Secure Live VM Migration in Cloud Computing: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 103 – No.2, October 2014.

[27] Antunes, N.; Vieira, M. Defending against web application vulnerabilities. Computer 2012.

[28] Nancy Arya, MukeshGidwani,Shailendra Kumar Gupta," Hypervisor Security - A Major Concern", International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 6 ,2013.

[29] E. S. Phalguna Krishna, E. Sandhya& M. Ganesh Karthik," Managing DDoS Attacks on Virtual Machines by Segregated Policy Management", Global Journal of Computer Science and Technology: E Network, Web & Security Volume 14 Issue 6 Version 1.0 Year 2014.