Cloud Computing: Attacks and Defenses

Omaji Samuel, Munan Ali Shah, Amir Hayat

Abstract— Cloud computing is described and considered to be a fast improving information technology which brought a new change and opportunity to the information technology world and in the field of human endeavor by providing environment for information and resources sharing that are delivered as a service to the final consumer over the World Wide Web on request. This could enable consumers to access and utilize their data at any point in time and also have beneficial online storage services. As a result of its numerous advantages, cloud computing is face with serious security risks. This paper reviews the research carried out in 2010-2014 and presents the classes of vulnerabilities of attacks in the cloud deployment models, their preventive measures and the performance evaluation on the types of deployment models.We also discovered a new attack surfaces on selected two deployment models describes in the section 6.3, which we recommended for future research work.

Index Terms— Cloud, Computing, Security Deployment, Model Architecture, Virtualization, Attacks and Defenses.

1 Introduction

THIS acceptance of cloud-based computing gives no result of retarding. In fact, the services of cloud are increasing at a geometrical rate touching all areas of the economy, with its sale for public cloud services was esti-mated to rise in the next decade. And there is no doubt that the cloud adaption is a convincing over for businesses and public organizations with similar interest, providing flexible access to shared, and simplify allocation of computing resources. The cloud model reduced the capital expenditures and minimizes the overhead costs of implementing a network, giving right for enterprise to concentrate more on their daily transaction instead on the IT provided by the cloud model. Conversely, the aim of cloud computing is to attract businesses in the aspect of resource sharing which provides an achieved economy of scale that can make the cloud model vulnerable to threat and attacks by the adversary [4].

The goal of cloud computing is to allow users to make tremendous use all of its technologies, without the need for deeper understanding about the technique embedded in them. Various organization rendering cloud computing products and services do not considered the implications of actually processing, storing and retrieval data in a common virtualized format. In reality, numerous designers of cloud-based applications manage to add protection, still as an addendum. In other cases, developers simply cannot provide tangible protection with recent reasonable technical strength.

Let's give a conceptual understanding of the research title, and to begin with the concept of cloud computing security, let simply say cloud safety; is a growing part of computer security; network security and diversely from information security, It has a wider scope of policies, technologies, and controls assigned to protect data, applications, and the affiliated infrastructure of cloud computing. Conversely, attacks can be view from the perspectives of an unauthorized access to a cloud environment, system or data and intentionally breaching the confidentiality, privacy, integrity, or availability of the cloud computing information system. Digesting the understanding of attacks, it is necessary to understand the defenses associated with this attacks, defenses is a way of preventing, suppressing intelligently the activity of an adversary with technical mechanism that will avert and restored the confidentiality, privacy, integrity of cloud computing world.

Having a written plan about what the cloud provider will do in a security event, such as a violation, is required by many regulatory standards. At the same time, many solution providers helping a client move to a cloud solution fail to spend enough time and effort to substantiate the offering's security. This may be because the client's primary reason for moving to the cloud is to reduce costs. Therefore, there may be little profit for the solution provider in the cloud relationship. These factors and the reality that cloud providers often silence clients into believing there's little reason to worry about security, make the role as a security solution provider even more difficult.

The ever-present use of cloud is so new that the National Institute for Standards in Technology (NIST), which is tasked with writing guidelines for proper use of technology, is only at the draft release stage with its cloud computing regulation. In a draft guiding principle on Security and Privacy in Public Cloud Comput-ing (800-144), released May 16, 2011, it is clear that even NIST members are rightfully concerned and cau-tious about the rapid and seemingly gratis move to cloud computing. As the document points out, "Many of the features that make cloud computing attractive, however, can also be at odds with traditional secu-rity models and controls" [6]. Still if one could show a degree of short-term cost savings in public cloud [7] versus client basis architectures, the risks considerably confront

- *Mr. Omaji Samuel is currently pursuing masters' degree program in Information Security in Comsats Institute of Information Technology, Islamabad Pakistan.*
  National Mathematical Centre, Kwali, Abuje, Nigeria.
  E-mail: omajiman1@gmail.com
- Dr. Munah Ali Shah is a lecturer at *Comsats Institute of Information Technology, Islamabad Pakistan.*
- Dr Amir Hayat is also a lecturer at *Comsats Institute of Information Technology, Islamabad Pakistan. Email: amir.hayat@comsats.edu.pk*

(This information is optional; change it according to your need.)

the prospective gains. There are considerable obstacles to securing data housed and controlled by an entity other than its owner, and this is improved with a public cloud, where communications, computing and storage resources are shared and data is often co-mingled [8].

In line with this development, we closely view cloud computing security on a very significant level, paying primary attention on attacks and hacking which are related to cloud computing providers and the systems [2]. Cloud computing are vulnerable to many attacks which has been an issue both in the past and in our comteporary time, many research work have being conducted to address the various attacks. This paper, is anticipating the classes of susceptibilities that is derived from cloud computing model; it shall provide preface attacks nomenclature for these, based on the understanding of cloud deployment components of the cloud. Security and Privacy should be given high priority and there is a need for high assurance and trust in order to create enabling arena of acceptance in the clouds ability to provide honest and consistent structure.

In Figure1. The deployment model architecture illustrate the layer of cloud service deployment, where the private cloud[9,10] gives a single cloud consumer's enterprise the exclusive privilege to the usage of infras-tructure and its computational resources, the public cloud[11], the cloud infrastructure and computing resources are made available to the general public over a public network and serves diverse pool of clients, the community cloud serve a group of cloud customers which have shared concerns such as mission objectives[12], security, privacy and compliance policy, rather than serving a single organization and it is implemented on the customer premises, lastly the hybrid cloud is the composition of two or more clouds(private on-site, community, off-site private[6], onsite community or public) that remain distinct entities but are bound together by standardized or proprietary technology that enables data and application portability[6,13,14] .Thus, each deployment model is vulnerable to different threats.

The rest of this paper will proceed as follow. Section 2 gives briefly the related work. Section 3 gives the different cloud models. Section 4 Recent work based on surface layer taxonomy vulnerability. Section 5 Review other surface attacks. Section 6 gives the cloud deployment taxonomy for cloud computing and its vulnerabilities of attack. Subsection of 6 shows the performance evaluation of deployment model and a table including surface attack on two cloud deployment models and finally Section 7 gives the conclusion.

2 Related work

2.1 Cloud Computing Attacks

In cloud computing, three major features such as confidentiality, integrity and availability (CIA) should not be breached. If the CIA is breached, the said cloud environment is susceptible to any form of attacks. When a cloud computing transmission or communication service has be compromise or modified in transit, then we say the cloud transmission has lost its integrity, similarly, when there is unauthorized destruction of data, and then we say that there is a breach of availability. Conversely, the unauthorized read of data can result to the breach of confidentiality. For synchronous transmission of information between the cloud service and the cloud client, a exceptional feature that require risk evaluation in areas such as integrity, privacy, recovery and evaluation of legal issues such as electronic discovery, regulatory compliance and auditing. We shall look at some potential cloud computing attack vectors which include [9]

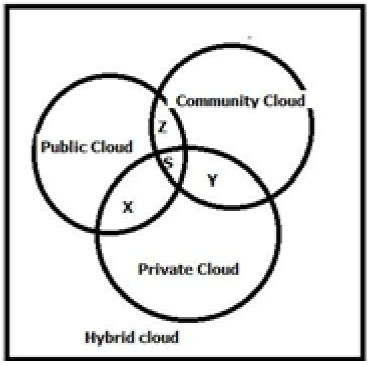

Fig.1. Gives the type Cloud Deployment Model embedded to form a hybrid cloud. The S-represent the cloud service provider, while x, y and z represents the various cloud deployments.

2.2 Network Issues in Cloud Computing

Recent studies now shows that most cloud computing transmission compromise is attribute to the denial of service. The cloud service server and its operating system notices the high work load on the flooded service, it will start to provide more computation power that is high service instances is needed to handle with the extra work load [6]. The hackers overflow the network server with recurrent demand of services to sabotage the network. The network server cannot legitimately grant the client regular requests [9]. For instance, the cyber criminals send thousands of requests to the cloud network server, thereby increasing its workload and this halt the functionality of the server from providing services to the legitimate clients. Providing a reduce privilege of client that connect to a server can reduce the DoS [15] attack. Other network security attacks are the meet in the middle attacks this is the kind of attacks where the secure socket layer (SSL) of a network is not con gure properly; communication link between two parties can be hijack by the middle or third party. Similarly, in network sniffing, this type of attack, here the data is not encrypted, thereby making it easy for attackers to compromise the data during communication. Port scanning; most internet port such as Port 80 (HTTP) is frequently available for web services to the client. Therefore port needed be secure by encrypting and ensure that the server software are con gure appropriately. Structural query language (SQL) injection and Cross Site channel is another type of cloud network attacks, unique characters to return the data for SQL scripting the request end up with a clause that might be change by inserting more information to it. The latter for which the user query a right universal resource location (URL) of a website and gain unauthorized access on other site to redirect the user to its own website and hacks its credentials [9].

2.3 Other Related Issues in Cloud Computing

The most vital features of cloud system are to improvise vigorous scalable resources. Cloud system continuously increasing in size when there is an additional requests from clients, cloud system initialize new service request in order to constantly meet the client requirements. Flooding attacks is mainly distributing a larger amount of twaddle requests to a particular service. When enormous amount of request is made, more resources cloud system will attempt to fight against the demand, and then the attackers attack the cloud server service. A prominence attack for web service is the XML signiture [15], it uses depend on a component name, attribute and value from illegal party but unable to protect the position in the documents. The attacker targets the component by running the SOAP [16] message and putting what he likes. Browser security is another attack; it is a situation where the requests to the server by web browser have to make use of secure shell layer (SSL) to encrypt the credentials to authen-ticate the user. If there is a middle party, the party can be able to decapsulate the data. If the hacker can runs a sniffing package on the targeted host, the hacker may obtain the credentials of the host and make use of these credentials in the cloud system as a legitimate user. The cloud malware injection [16] attack is another attack which aim is to damage a service, applications or virtual machine. An intruder is oblige to generate his personal nasty applications, service or virtual machine request and put it into the cloud system [9].

3 The Different Cloud Models

Different cloud models have been designed to identified the major facets, their activities and function in the cloud computing. The cloud computing reference model gives the generic view of all the facets of the cloud computing components [6]. Each facet is an entity that participates in the dealing or processing and carry out tasks in cloud computing.

3.1. The deployment model

A cloud computing system can be implemented privately, or hosted on the premises of a cloud customer which may be shared among a few number of agreed partners. Likewise, may be housed by a third party or may be made publicly for the general accessibility of services. Depends on the various cloud deployment used, customers may monitor their resources, provide scalabilities, cost and availability [14].

3.2. Cloud Service

The cloud can afford access to software applications such as email, office productivity tools (Software as a Service, (SaaS) service model), or can provide an enabling environment for clients to implement and operate their own software (Platform as a Service, (PaaS), service model) or can lease network access to conventional computing resources such as a processing power and storage (Infrastructure as a Service (IaaS), service model). The various service models satisfies customer according their various business objectives [14].

4 Recent work based on surface layer taxanomy vulnerabilities

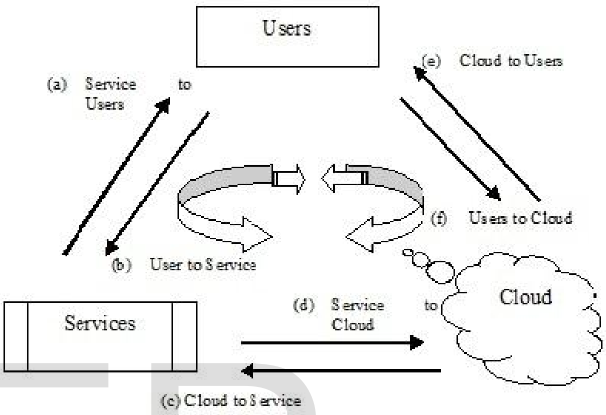

Fig.2. the diagram above illustrates the cloud surface attacks. The arrows describe the pattern of interactions among the attack surfaces, resulting into the six attacks surfaces explained below.

In many cloud computing scenarios, various models using three classification of layer: the service users, the service instances and the cloud provider. This scenarios form a circular relationship of the classes of surface attack.[2]. In this paper we shall briefly explained the six surface attack taxonomy which are;(a) service-to-user, all attacks are possible in this surface, since it exhibit the client-service infrastructures this include attacks like buffer overflow, SQL injection or privilege escalation (b) User-to- service; here the client program uses a server such as browser which has related attacks for the hypertext markup language(HTML) based services like secure shell (SSL) certificate spoofing, attacks on browser cache or phishing attacks on mail clients are the common attacks on the user-to-server surface attacks. (c) Cloud-to- service; the parting of service instances and cloud provider can be risky, cloud attack surface to the service instances can run in aligned with it host on the cloud system. Attacks include the exhaustion attacks, triggering the cloud provider more resources or end up in a denial of service or attack on the cloud system hypervisor. (d) Service-to-cloud; it incorporate all virtually all forms of attacks that a cloud provider can perform against a service running on it. Privacy related attacks, malicious interference; this is the most crucial attacks surface compare to other surfaces. (e) Cloud-to- user; these usually do not have real touching points. And lastly the (f) user-to-cloud surface, here attacks involves phishing like activities that activate a client into manipulating it cloud provided services and involves every kinds of attacks that target users and originate at the cloud system.

5 Other surface attacks

Attacks surface exposed by your environment can cause vulnerability for an adversary to launch an attack. some of the surface seem hard to implement especially the Virtual machine (Hypervisor Manager attacks) which could result to escape the virtual machine (VM) attack or Virtual switch (vswitch attack) as all known layer 2 attack against switching fabric are migrated by using virtual switches.

3.1. Virual Level Attack

Vulnerability attacks in hypervisor VM is used by cloud vendors which are a potential in multi-tenant setting. When provided with computing resources from the cloud in the form of VMs, subscribers should make ensure that the cloud provider has mechanism to protect against VM attacks on the same physical host, or the physical host itself [14]. The possibilities of attacks surface are Denial of Service (DoS) [9], this occur as a result where VMs is overload with processes from the multi-tenants.

Client-client attacks, occur when a spiteful VM could infect all VMs that exist in the physical server [13]. An attack on a single client VM can escalate to other VM's that is housed by the same physical host; this is the worst security risk in virtualized environment [16]. The attacker gets the administrator right on the infrastructural [17] level or virtualization environment and then can own all data transmitting between VM and Hyper-visor and can perform Spoofing Attacks [18]. A distinctive attacks discovery and preventive mechanism includes virtual firewalls. Virtual intrusion detection scheme and the intrusion prevention technique IDS/IPs, and some network segmentation techniques such as Virtual Local Area Network (VLAN)[6] should be implemented. From the table 1 below in the next subsection, this paper describes some other possible surface attacks in cloud computing.

6 Cloud deployment taxanomy for cloud computing and its vulneralability of attacks

Cloud deployment is one the key component of cloud computing. There are number of methodologies and ways to defined component of a cloud. There is no clearly definition or standard [4]. Therefore, there is several understanding of deployment models with no one being better defined than another. Deployment can be described as process of providing availability of resources, be it software. Deployment model in cloud computing are the private cloud, public cloud, community cloud and the hybrid cloud [6]. Depending on the types of computing being considered, an organization might use either a public or private cloud space as attest bed to gain experience and capability before moving around. Clients need to do and thoroughly study of the providers with regard to security, government, risk and compliance. Choosing the right models involves a swapping between the perceived benefits and the perceived risks. Risks of multi-leasing, the workload of variegated users may reside concurrently on the same system and local network separate only by access policies implemented by a cloud provider and operation policies and procedures could compromise the security of the consumers.

The security threats in on-premises in the deployment model can be applicable to all the types of cloud deployment model used the protection of cloud resources using strong security perimeters [6] against internal and external threats, for low impact data and processing the security perimeters rewalls, set virtual private network (VPN).[13] For higher impact data the more restrictive firewall policies, multifactor authentication, encryption, instruction detection and prevention and even physical isolation[14]. The security threats in on premises, the security perimeters needs to be implemented on both consumer's premises and the provider's premises and the communication channels is required to be secured. The vulnerabilities of the two cloud deployment model as follows: Public cloud surface attacks which involves; cloud provider, co-tenants and users. The private cloud surface attack involves; Cloud provider (if managed) and users.

6.1 Deployment Model Surface Attack

The public cloud surface attacks are the types of surface attacks that follow the scenario of the surface attack taxonomy. Here the adversaries uses the vulnerability of the cloud provider, co-tenants and the user surface to lunch all the six surface attacks. The counter measures are to ensure that the surfaces are difficult for the attacker to attack. We use [2] counter measures against any surface attacks. The possible vulnerability of attacks in the co-tenants surface is likely to be the denial of service (DoS); the counter measure is to restrict the privileges of large number of request to the cloud server. Others include man-in-the middle attacks, side channel, their possible measures include the possibility of com-munication path interception should be highly secure using the Secure shell layer (SSL) should be properly run and checked prior to communicating with the legitimate parties. Conversely, the universal resource lo-cator (URL) of the website should be encrypt and its credential hidden from any adversary. The user's surface is also vulnerable to the following network attacks as illustrated in subsection 2.2. Counter measures includes, properly install rewall to prevent port attacks, ensured encrypted method of securing data against network sniffing attacks on data. The intrusion detection system is needed to sieve the malicious request by installing rewall to prevent flooding attacks, authenticity check for received messages using the hash function mechanism for all upcoming requests to prevent the cloud malware injection attacks.

Similarly the private cloud deployment has the following surfaces; cloud provider if not properly managed and the user. Here the co-tenants in excluded because the private cloud in managed by organization or individual and does not required the utilization of the general public, hence the co-tenants surface attacks is not applicable to the private cloud. The various preventive measure discussed in the public cloud attack surface can be applied to the private cloud exception of the co-tenant susceptible attacks. You can infer from the appendix 8 in the last page of this paper that the interaction of the two deployment model consider in section 4 of this paper which depict the idea obtained in the above section.

Table 1 Other Cloud Surface Attack

ATTACK SURFACE	PLATFORM	TYPES OF THREAT	DEFENSES
Tenant Portal	Cloud Service[6,36]	All network attacks[9,28]	Install,Firewalls[9],Accountability check[25]
Management	Cloud Provider[6,2,36]	Insider Attacks[31]	(a) Encryption of data to prevent rogue Administrator [31]. (b) Data authentication against cloud exploits.[31] (c) Install firewall proxies against those using cloud against you.[31]
Applications/IaaS	Cloud Service	Network,other security issues[9,14] and computer viruses	Install firewalls,Intrusion detection system,digital Certificate and encryption [28, 9], Install antivirus.
OS/PaaS			
Escape the VM	Hypervisor [14,16,31,28]	Denial of service (DoS)[6],Spoofing [9]	Virtual Firewall[16], Virtual IDS/IPs, Network segmentation technique and VLANs[13,6,31]
Vswitch Attacks			Install antivirus to prevent Bootsector computer virus.
Storage Attacks	Cloud Service[6,2,36]		Effective storage scheme,
Physical Environment Attacks	Deployment[6]	Insider[31],Natural disaster and Theft	Provide authentication to denial access to unauthorized users, proper security perimeters[10], policies and Regulatory standard.

The *other clouds surface attacks*

6.2. Performance Evaluation of Deployment Model

The evaluation and performance of the two cloud deployment model will be considered in the paper. The evaluation ranges from the three fundamental facets in cloud computing which include; the cloud provider, the cloud service and the cloud users. Taking the general look at the performance which include the workload and infrastructure [25],the security is [24,25], with reduced latency in the private cloud environment, this is because transversal of the public internet to the end storage performance in private cloud environment with the use of high performance storage hardware and configuration of high bandwidth connectivity to these devices. The cost of [24,25] is less in private cloud on a VM per hour (operational expenses) basis compared to a public cloud and storage network cost will most likely reduced significantly. The table 2 below in the next sub-section of the performance evaluation of the deployment model gives you the over view of the necessary parameters needed when implementing deployment model in cloud computing.

6.3. Proposed Model

The figure below shows the chain between the two cloud deployment models and the cloud service provider. The vulnerabilities of the attacks follows the pattern of the six surface attacks explained in section 4 of this paper.

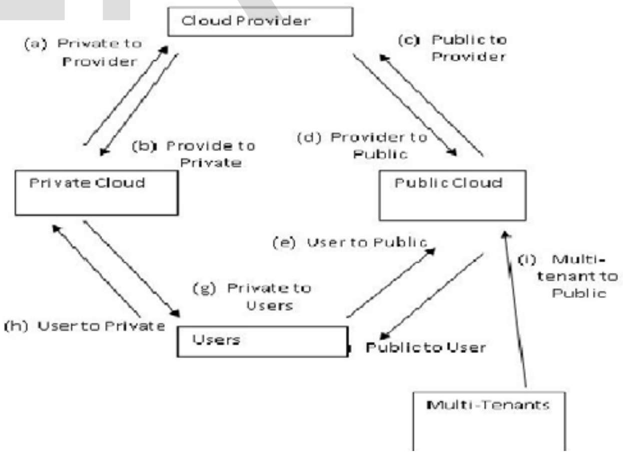

Fig.3. the cloud computing deployment model surface attacks

for private and public cloud.

Table 2 the Performance Evaluations of the Different Deployment Models, Attacks, and Solutions That Exist In Their Respective Surfaces

	INFRASTRUCTURE	CLOUD	SERVICES	USERS	ATTACK SURFACE	ATTACKS	PERFORMANCE
Public Cloud	Third Party[6]	Third Party[6]	Off Premises[29]	All or untrusted	a. Cloud Provider b. Co-tenant c. Users	Denial of services(occur most frequently) and all other attacks	a. Workload: high b. Security: Low c. Latency: High d. Cost: less expensive[24]
Private cloud	Organization[6]	Organization or third party[10]	On premises or off premises[29]	Organization[17]	a. Cloud provider(if managed) b. Users	(Insider attacks most likely)[23] occur most frequently and all other attacks	a. Workload: reduced(High performance CPUs) b. Security: High c. Latency: Reduced d. Cost: very expensive [30]
Community cloud	Organization [17]	Organization or third party[17]	On premises and off premises	Organization [6]	Applicable as with private cloud	Some Attacks as in private cloud	
Hybrid cloud	Organization and third party[17]	Organization and third party[17]	Both on premises and off premises	Both trusted and untrusted [17]	Applicable with both private and public cloud	All attacks[13]	

7 Conclusion

Cloud computing helps IT enterprises with various technologies to optimize and secure application performance in a low cost manner. Cloud provider often have several powerful server and resources in order to provide appropriate services for their prospective customers. But cloud is at risk similar to other network based technology. In addendum, the vulnerability of attacks can be classified based on the knowledge of the cloud deployment model paradigm. Cloud deployment model surface attacks for public and private cloud and their countermeasures are discussed in this paper. It has several models to prevent it data and resources from an ad-versary and to provide optimum services to the users. The notion of the deployment model surface attack will enable prospective individual or organization that are willing to setup cloud computing technology through the understanding of the classes of vulnerabilities of cloud-based attacks on surface deployment model.

In this paper, we have shown the performance evaluation for two cloud deployment model, we do not dis-cuss the deployment model for community cloud and hybrid cloud computing, it is therefore recommended for further study. Being a new exploration, our new model in the appendix, we were able to classify the cloud model discussed and recommend for future work and we also associated with it our discovered surface attacks. We continuously collect and classify the susceptibilities of attacks neither to ascertain nor contradict our categorization's applicability and suitability.

Acknowledgment

The author wish to thank Comsats Institute of technology, Islmabad and National Mathematical Centre, Abuja, Nigeria.

REFERENCES

[1] Ashley Chonka, Yang Xlang, Wanlei and Zhou Alessco Bonti. Cloud Security Defeonce to Protect Cloud Computing Against HTTP-DoS and XML-DoS Attacks. Journal of Network and Computer Applications, vol.34. pp.1097-1107, July 2011

[2] A. Singh and M. Shrivastava. "Overview of Attacks on Cloud Computing". *International Journal of Engineering and Innovative Technology (IJEIT),* vol.1, pp. 321-323, 2012.

[3] Behi .A. "Emerging Security Challenges in Cloud Com-puting: An Insight to Cloud Security Challenges and Mitigation." *Information and Communication Technology (WICT),* 2011, (World press)

[4] How Cybercriminals Attack The Cloud Dark Reading. [Online]. Avaiilable Online http://www.darkreading.com/attacksbreaches/howcybercriminals-attack-the-cloud/240153610.

[5] Shaikh, F.B.Haider, S. "Security threats in cloud computing". Internet Technology and Secured Transactions (ICITST), pp.214-215, 2011.

[6] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger,D. Leaf." NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and Technologies". dl.acm.org Special Publication (500-292) ,2012

[7] Joshi.B. Vijayan.A.S., Joshi.B.K. "Securing Cloud Computing Evironment against DDoS Attacks". *Computer Communication and Informatics (ICCCI),* pp.1-5, 2012, (IEEE Publisher).

[8] Amanatullah, Y. Lim, C. Ipung, H.P. Juliandri, A. "Toward cloud computing reference architecture: Cloud service management perspective" *ICT for Smart Society (ICISS)*, pp.1-4, 2013.

[9] H.I. Sara Qaisar. "Cloud Computing: Network/Security Threats and Countermeasures", *Interdiscip. J. Comtem-porary Res. Bus.*, vol. 2, No 9. 2012.

[10] MD.Tanzim Khorshed, A.B.M. Shawkat Ali and Saleh.A. Wasimi A "Survey on Gaps, Threats Remendiation Challenges and Some Thoughts for Proactive Attack Detec-tion in Cloud Computing"*. In Future Generation Com-puter System,* vol. 28, pp. 833-851, 2012. (Elsevier Publisher).

[11] S. O. Kuyoro." Cloud Computing Security Issues and Challenges". *International Journal of Computer Networks,* no. 3, pp. 247-255, 2011

[12] N. Vijaykumar. "Seedling Clouds with Trust Authors". *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, pp. 43-46, 2010.

[13] CC Synopsis. NIST Special Publication, 2012.

[14] L. Badger, R. Pattcorner, and J. Voas. "Cloud Comput-ing Synopsis and Recommendations of the National Institute of Standards and Technology". In dl.acm.org, 2012.

[15] Kai.Hwang and Deyi Li. T"rusted Cloud Computing with Secure Resources and Data Coloring". *Internet Computing,* vol.4, pp.14-22. 2010. (IEEE Publisher)

[16] Susan .V. V and Kazi Zunnurhain. "Security Attacks and Solutions in Clouds". *Proceedings of the 1st international conference*, 2010.

[17] J.Du, N Shah and X.Gu. "Adaptive Data-Driven Service intergrity Attestation for Multi-Tenant Cloud" *Proceed-ings of the Nineteenth International Workshop on Quality of Service*, dl.acm.org, 2011.

[18] What-is-new-cloud-security.pdf[online]Avalable:http: www.utdallas.edu

[19] G. Zhao, C. Rong. M. G. Jaatun, F.E Sandnes. "Deployment Model: Towards Eliminatiing Security Concerns from Cloud Computing". *International Conference on High Performance Computing and Simulation*, pp 189-195, 2010.

[20] Qiang Guan, Chi-Chen Chiu, Song Fu. "CDA: A Cloud Dependability Analysis Framework for Characterizing System Dependability in Cloud Computing Infrastructures". Dependable Computing (PRDC), IEEE 18th Pacific Rim International Symposium, pp.11-20, 2012.

[21] Sabahi. F. "Cloud Computing Security Threats and Responses". *Communication Software and Networks (ICCSN)*, pp. 245-249, 2011.

[22] M. K Srinivasan and P. Rodrigues. "State of the art Cloud Computing Security Taxanomies: A classication of security Challenges in the present Cloud". *Proceedings of the International Conference on Advances in Com-puting, Communications and Informatics*, dl.acm.org, pp.470-476, 2012.

[23] Wentao Liu. "Research on cloud computing security prob-lem and strategy"*. Consumer Electronics, Communications and Networks (CECNet), 2nd International Conference*, pp.1216-1219, 2012.

[24] R. Tudoran, A. Costan, G. Antoniu and L. Bouge. "A Performance evaluation of Azure and Nimbus Clouds for Scientific Applications "*Proc. 2nd International Workshop Cloud Computing Platform-CloudCP, pp*. 1-6, 2012.

[25] Zaki Hassan, S.A. SONA: "A service oriented nodes architecture for developing Cloud Computing applications". *Advanced Computing and Communication Sys-tems (ICACCS), International Conference*, pp. 1-6, 2013.

[26] S. P Mirashe and N. V. Kalyankar. "Cloud Computing Communication "ACM, vol.51, no.7, pp. 9, 2010.

[27] G.T. Office. Cloud Security and Risk Management, 2011.

[28] Qingjie Meng, Changqing Gong. "Research of cloud computing security in digital library Information Management". *Innovation Management and Industrial Engineering (ICIII), 6th International Conference*, vol. 1, pp. 41-44, 2013.

[29] Subashini.S, V. Kaviitha. "A Survey on Security Issues in Service Delivery Models of Cloud Computing". Journal in Network Computing Applications Vol.34, pp. 1-11, 2011.

[30] B. Adler. "Designing Private and Hybrid Clouds ", *RightScale Inc*, 2012.

[31] W.R. Claycomb and A. Nicoll. "Computing: Directions for New Research Challenges". *IEEE 36th Annual Computer Software Application Conference.*, pp.387-394, 2012.

[32] S. Ramgovind, E. Mm and E. Smith." The Management of Security in CLoud Computing", *Information Security for South Africa (ISSA)* pp. 1-7, 2010.

[33] W. Jansen and T. Grance. "Guidlines on Security and Privacy in Public Cloud Computing", 2011, (NIST special publication).

[34] K. Chadha. "Security Aspect in Cloud Computing", *International Journal of Computer Applications v*ol.40 no.8, pp.43-47, 2012.

[35] Yildirim, A.S. and Girici, T. "Cloud Technology and Performance Improvement with Intservice over Different service for Cloud Computing". *Future Internet of Things and Cloud (FiCloud),* pp. 222-229, 2014.

[36] Comparing Public, Private, and Hybrid Cloud Com-puting Options - For Dummies. [Online]. Available: http://www.dummies.com/how-to/content/comparing-public-private-and-hybrid-cloud-computin.html., Acessed in 2013.

[37] Jadeja, Y. Modi, K. "Cloud computing concepts, architecture and challenges. Computing", *Electronics and Electrical Technologies (ICCEET)*, pp.877-880, 2012.