International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 4 2393 - 2397

Security Threats of Cloud Computing

Nancy Awadallah
Department of Computer and Information Systems
Sadat Academy for Management Sciences
Mansoura ,Egypt
rarecore2002@yahoo.com

***Abstract*—** Cloud computing presents a convenient environment and more advantages to business organizations to run their business, it's benefits aims to make the location computing infrastructure shifted to the network in order to reduce the costs of hardware and software resources maintenance, also it offers the processing power and the computing resources of geographically distanced computers connected via internet. It has advantages such as outsourcing, scalability, efficiency, resilience, and non-core activities and flexibility. In this paper, cloud service models and deployment were introduced; cloud security challenges were investigated based on the cloud service models nature. Also this paper seeks to address various threats which face cloud computing and the possible solutions to demonstrate the techniques that hackers used against.

Keywords- *Cloud Computing, Infrastructure, Security, Trust, Confidentiality .*

*****

I. INTRODUCTION

Cloud computing is Internet-based computing, whereby shared information, resources and software are provided to computers and other devices on-demand. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. It refers to accessing computing resources that are typically owned and operated by a third-party provider on a consolidated basis in data center locations. Also it is considered a style of computing in which scalable and virtualized resources are provided over the internet as a service.

The difference between cloud and other computing such as utility computing and grid computing that the later is a form of parallel and distributed computing, in which virtual and super computer' is composed of a cluster of networked, such as coupled computers acting together to perform large tasks, but cloud computing is considered the packaging of computing resources as a metered service.

Cloud computing characteristics include rapid elasticity, on-demand self service, resource pooling, wide network access and measured service. On-demand self service means that customers can request and manage their own computing resources. Wide Pooled resources means that customers draw from a pool of computing resources, usually in remote data centres. Network access allows services to be offered over the Internet or private networks. Services can be scaled larger or smaller, and use of a service is measured and customers are billed accordingly.

While there are benefits, there are privacy and security concerns too. Data is travelling over the Internet and is stored in remote locations. In addition, cloud providers often serve multiple customers simultaneously. All of this may raise the scale of exposure to possible breaches, both accidental and deliberate.

Concerns have been raised by many that cloud computing may lead to "function creep" — uses of data by cloud providers that were not anticipated when the information was originally collected and for which consent has typically not been obtained. Given how inexpensive it is to keep data, there is little incentive to remove the information from the cloud and more reasons to find other things to do with it.

The following section focus on a previous studies on security issues in cloud computing and the rest of sections are organized as follows. Section II presents security issues of cloud computing. Section III introduces cloud computing infrastructure deployment and service models. Section V deliberates on associated cloud computing security and challenges and the last section presents suggestions to privacy issues.

II. PREVIOUS WORKS

Kuyoro S. O. et al. [1] presented an analysis study of the cloud computing challenges and security issues especially on its types and the types of service delivery.

S.Hashemi [2] suggested how to increase trust and enhance using cloud computing as it is technology has a value among people. This technology will make improving in security to be better by providers.

A. Ukil et al. [3] explored issues of security and the challenges concerns of cloud computing new solutions. They proposed architecture for merging different cloud computing security techniques and protocols, such as Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) systems. It will facilitate the cloud system managing more effectively and

provide the specific solution to counter the threat for the administrator. They used experimental data to show how a cloud service provider can estimate the charging based on the security service it provides.

S. Suakanto et al . [4], conducted an experimental setup to measure the quality of service received by cloud computing customers. Experimental setup done by creating a HTTP service that runs in the cloud computing infrastructure. They interested to know about the impact of increasing the number of users on the average quality received by users. The qualities received by user measured within two parameters consist of average response times and the number of requests time out. Experimental results of this study show that increasing the number of users has increased the average response time. Similarly, the number of request time out increasing with increasing number of users. It means that the qualities of service received by user are decreasing also. They found that the impact of the number of users on the quality of service is no longer in linear trend. The results of this study can be used as a reference model for the network operator in performing services in which a certain number of users in order to obtain optimal quality services.

D. C. Wyld [5] , examined non-military uses of cloud computing in governments across the globe, from the Unites States to Europe and Asia.

F. Arabalidousti et al . [6] , Proposed a Comprehensive Cloud Architecture, which based On The It Service Management Frameworks, Reference Models And Cloud Architectures To deliver better Services In Cloud Computing Environment.

F. S. Gharehchopogh et al . [7] , provided strategies for solving related issues and problem of data security which is the main goal of sub-structures in cloud computing.

III. CLOUD COMPUTING INFRASTRUCTURE

Cloud computing is considered convenient, network access for sharing computing resources that can be released rapidly and provisioned with minimal effort of management or interaction of service provider [8].

A. Cloud Deployment Models

Cloud computing development models include the aim and identity of cloud and the method which are settled.

The following four types of the development models according to NIST definition:

- **Public cloud:** also called external cloud which describes the mainstream sense of cloud computing, how resources are provisioned via web services, self-service basis over the internet, from a third-party off-site provider who shares resources [9]. Large Cloud Service Provider (CSP) managed the infrastructure of cloud.

- **Private cloud:** is only used for an organization, accessing data , applications and services are available for everyone in the organization but others out of organization can't do that[9].

- **Community cloud:** when several organizations have similar requirements to share infrastructure, this model is used. Community cloud examples include Google's "Gov Cloud". Security needs are supported in this model [10].

- **Hybrid cloud:** is combination of two or more clouds .It allow organizations to optimize their resources, so the critical core activities can be run under the control of the private component of the hybrid cloud while other additional tasks may be outsourced to the public component [9].

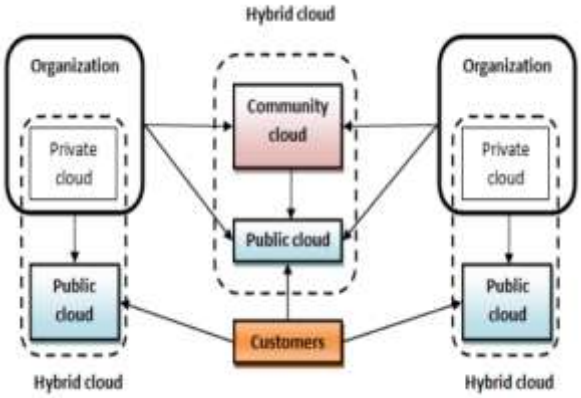

Figure. 1 Cloud Computing Deployment Models

B. Cloud Service Delivery Models

Three fundamental service models are offered by cloud computing providers such as: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS):

- **SaaS.** The services provided by SaaS include using functional programs on the infrastructure of cloud and access through the web browser [11]. The infra-structure of cloud including customers operational systems, servers and saving area are not managed by customers [10].

- **PaaS.** The difference between the PaaS and SaaS is that the first includes exclusive program environment and computing platform, developing and solution strategies.

- **IaaS.** This kind of service saving space [10]. The management or control in infra-structure not be done by the client but has control over the operation system. In this service an artificial server is available for the client [11][12].

The hierarchy of cloud-based services allows selecting the level of services which are appropriate for the challenges of their specific business. Solution may encompass all tiers if the

complexity level grows, and business process may be offered as a service.

Figure. 2 illustrates the infrastructure layers within the cloud.

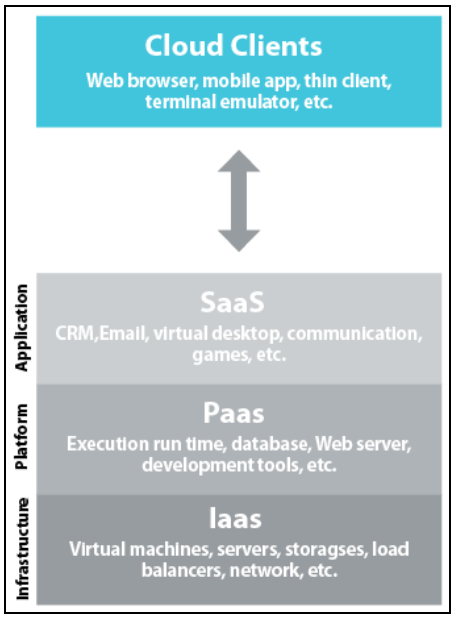

Figure. 2 Cloud Computing Infrastructure

IV. CLOUD SECURITY ATTACKS

User level threats, network Level and threats at CSP level are considered security threats at different levels. Dealing with These threats should be taken to keep the cloud up and running continuously.

A. Cloud Service Provider (CSP) Level Attacks

The vulnerabilities of cloud computing should be considered by end users before migrating to it. Sharing resources such as network, computing capacity and storage are such examples. Many security breaches are listed below:

- **Guest-hopping attack:** trying getting access to one virtual machine by an attacker who hacked another virtual machine hosted in the same hardware.
- **SQL injection:** the most famous method of websites attacking. It's methodology for executing by injecting SQL commands into a database of an application from the web to evacuate or breakdown that database.
- **Side channel attack:** on the same physical machine, the attacker places a malicious virtual machine as the victim machine; the attacker can access all the private "sensitive "information on this victim machine.
- **Malicious Insider :** One of the cloud computing challenges located at the data centers of the service providers is when its employee is granted access to sensitive data of some or all customers administrators.

B. Network Level Security attack

These attacks may be done from users outside the cloud, it is defined as (a user seek to attack the cloud for any purpose), or a malicious insider hiding between the user and the CSP and trying to disrupt the data to/from the cloud.

- **Domain Name System (DNS) attacks:** converts host names into corresponding Internet Protocol (IP) addresses using a distributed database scheme. Internet DNS servers are subject to different types of attacks such as: ARP cache poisoning domain hijacking, and man-in-the-middle attacks.
- **Domain hijacking:** Is defined as changing the name of a domain without the knowledge or permission from the domain's owner or creator. Domain hijacking enables intruders to access sensitive corporate information and perform illegal activity such as phishing, where a website is replaced by an identical website that records private information.
- **IP Spoofing:** Is where the attacker gains unauthorized access to a computer by pretending that the traffic has originated form a legitimate computer. IP spoofing is utilized to make other attacks such as Denial of Service attack and Man in The Middle attack.[13]

C. End users' attacks

Most of the cloud users' attacks are phishing, fraud, and exploitation of software vulnerabilities still work and can threaten the cloud service infrastructure.[14]

V. SECURITY IN CLOUD COMPUTING

The Security issue is the most important aspect for cloud system due to its nature of outsourced computing. Without robust security scheme and user-centric security policy is implemented, cloud system would be vulnerable to different attacks and susceptible by the users. As the cloud computing approach could be associated with having users' sensitive data stored both at clients' end as well as in cloud servers, especially confidentiality, integrity and authentication are the primary pain areas in cloud computing.

To create substantially secure cloud computing environment, it is required exploring the challenges and issues of security in cloud computing like:

• To provide data confidentiality for clients / cloud users. • To enable cloud information integrity. • To ensure application independent single sign-on (SSO) kind of authentication.

Confidentiality prevents intentional (malicious) or unintentional disclosure of sensitive information. In cloud

systems, confidentiality incorporates data encryption to minimize vulnerability due to covert channels, traffic analysis, and sensitive inference. Malicious activities can be defended through a protected hypervisor through HyperWall architecture using the concept of hardware centric hypervisor-secure virtualization [15][16].
For guaranteeing data integrity at rest or storage, particularly in IaaS and PaaS systems, trusted infrastructure needs to be incorporated. For data integrity in transit, traditional digital signature can be used [17].

The security challenges for cloud computing approach are somewhat dynamic and vast; some of these challenges are abstracted as following:

D. Data location

Data location is a vital factor in cloud computing security [18]. Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated. Cloud users' personal data security is thus a vital concern in a cloud computing environment. In terms of customers' personal or business data security, the strategic policies of the cloud providers are of highest significance as the technical security solely is not adequate to address the problem [19][20].

E. Trust

Trust is another problem which raises security concerns to use cloud service for the reason that it is directly related to the credibility and authenticity of the cloud service providers. The provision of trust model is essential in cloud computing as this is a common interest area for all stakeholders for any given cloud computing scenario. Trust in cloud might be dependent on a number of factors among which some are automation management, human factors, processes and policies. Trust in cloud is not a technical security issue [21], but it is the most influential soft factor that is driven by security issues inherent in cloud computing to a great extent [2][20].

All kinds of attacks that are applicable to a computer network and the data in transit equally applies to cloud based services some threats in this category are man-in-the-middle attack, phishing, eavesdropping, sniffing and other similar attacks as illustrated in previous section. DDoS (Distributed Denial of Service) attack is one common yet major attack for cloud computing infrastructure .The well known DDoS attack can be a potential problem for cloud computing, though not with any exception of having no option to mitigate this [22]. The security of virtual machine will define the integrity and level of security of a cloud environment to greater extent.

F. Authentication

Verification of eligible users' credentials and protecting such credentials are part of main security issues in the cloud violation in these areas could lead to undetected security breach at least to some extent for some period.
As well as using encryption falls within the practice of safe computing - they can be well considered as part of security concerns for cloud computing. However, it is important to distinguish between risk and security concerns in this regard.
Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities. Like any other network scenario, the provision of insider-attack remains as a valid threat for cloud computing. Any security tools or other kinds of software used in a cloud environment might have security loopholes which in turn would pose security risks to the cloud infrastructure itself. The problem with third party APIs as well as spammers are threats to the cloud environment [18].

VI. SUGGESTIONS TO PRIVACY ISSUES

In this section, there are many suggestions for cloud user and cloud providers according to cloud computing privacy issues.

A. For Cloud User

These suggestions are given to the cloud user when placing their data in the Cloud Provider. The cloud user should carefully read the privacy policy before placing their information in the cloud. If a cloud user doesn't understand any of the policies, it should be clarified with the provider or may consider other service providers [23].
Cloud user must have a close attention regarding rights to use, disclose, or make public cloud user information.
Suppose the cloud user wants to remove any data from the cloud, the cloud provider must take necessary steps to remove the data. The Cloud user has rights to check whether that data is still retained by the cloud provider.
Cloud users should not place any important data which may be helpful for their competitors, government and others.
Cloud users mustal ways have a consultation with their technical support group about the advisability of keeping their data in the cloud.

B. For Cloud Providers

The following suggestions are for the providers to maintain the cloud user's data in the Cloud.

- Cloud provider must ensure that they are not violating any law or policy.
- Cloud Provider should mention the physical location of the cloud user's data in the cloud
- Cloud Provider should maintain the isolation between different user's data.
- Protection mechanism of cloud must be known to the user.
- Recovery plans are to be mentioned by the provider in case of natural disaster.
- Cloud Provider must list the various laws and regulations that govern the cloud user's data.
- Cloud users must be given advance notice to the changes of the privacy policies
- Periodically, the provider should conduct the audit trails and maintain log of user's data.

VII. "CONCLUSIONS

Cloud computing will promote the use of shared resources and when we are sharing the resources among different users it will definitely lower the costs and will help in keeping the environment clean .In this paper key security considerations and challenges which are currently faced in the cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. It assumes to address challenges to provide data confidentiality for clients / cloud users, to enable cloud information integrity and to ensure authentication. This paper describes the problems on data confidentiality, data integrity and data authentication and our security concern aims at the cloud user perspective. In cloud computing, cloud users or clients are most vulnerable to different security threats.

REFERENCES

[1] Kuyoro S. O., Ibikunle F. & Awodele O.,"Cloud Computing Security Issues and Challenges ", International Journal of Computer Networks (IJCN), Volume (3) , Issue (5), 2011.

[2] S.Hashemi ,"Cloud computing technology: Security and Trust Challenges ", International Journal of Security, Privacy and Trust Management (IJSPTM) , Vol 2, No 5, October 2013.

[3] A. Ukil , D. Jana and A.D. Sarkar ,"A security framework in cloud computing infrastructure ", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013 .

[4] S. Suakanto , S. H. Supangkat , Suhardi , R. Saragih ,"Performance measurement of cloud computing services ",International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.2, April 2012.

[5] D. C. Wyld,"The cloudy future of government IT: Cloud computing and the public sector around the world ",International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1, January 2010 .

[6] F. Arabalidousti, R. Nasiri ,M. R. Davoudi , "Developing a new architecture to improve ITSM on cloud computing environment" , International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol. 4, No. 1, February 2014 .

[7] F. S. Gharehchopogh, M.Bahari, "Evaluation of the data security methods In cloud computing environments " , International Journal in Foundations of Computer Science & Technology (IJFCST), Vol. 3, No.2, March 2013.

[8] M. Firdhous, O. Ghazali, and S. Hassan, Trust and Trust Management in Cloud Computing – A Survey, Inter Networks Research Group, University Utara Malaysia, Technical Report UUM/CAS/InterNetWorks/TR2011-01, 2011.

[9] D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science and Technology, Vol. 3, No. 4, p. 2672-2676, 2011.

[10] S. Qaisar, K.F. Khawaja, " Cloud Computing: Network/Security Threats and Countermeasures", Interdisciplinary journal of contemporary research in business, Vol.3, No 9, p. 1323-1329, 2011.

[11] J.R. Winkler, " Securing the Cloud: Cloud Computer Security Techniques and Tactics", Technical EditorBill Meine, Elsevier Publishing, 2011.

[12] N. M. Turab, , A. A. Taleb , S. R. Masadeh ,"Cloud Computing Challenges and Solutions", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.5, September 2013.

[13] B. R. Kandukuri, R. V. Paturi , A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference onServices Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. 2009. ISBN: 978-0-7695-3811-2

[14] Klaus Pl¨ossl, H. Federrath, , T. Nowey , "Protection Mechanisms against Phishing Attacks" http://www-sec.uni-regensburg.de/publ/2005/PlFN2005Trust Bus05Phishing.pdf

[15] Y., L., Rong, C., Zhao G, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography,"CloudCom, pp167–177, 2009.

[16] Szefer, J. Lee, R.B. Ruby & B. Lee, "Architectural Support for Hypervisor-Secure Virtualization," I 7th International Conference on Architectural Support for Programming Languages and Operating System, pp437 – 450, 2012.

[17] Ukil, A.,Sen, J., Koilakonda S, "Embedded Security for Internet of Things," 2nd IEEE National Conference on Emerging Trends and Applications in Computer Science, pp1-6 , 2011 .

[18] M. Ahmed ,M. A. Hossain, "Cloud Computing And Security Issues In The Cloud " , International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 .

[19] Teneyuca, D. ,"Internet cloud security: The illusion of inclusion. Information Security Technical Report ", 16, 102-107. doi:10.1016/j.istr.2011.08.005, 2011.

[20] Ryan, P. and Falvey, S., "Trust in the clouds. Computer Law and Security Reviews ", 28, 513521. http://dx.doi.org/10.1016/j.clsr.2012.07.002 , 2012.

[21] Abbadi, I.M. and Martin, A," Trust in the Cloud. Information Security Technical Report", 16, 108-114. doi:10.1016/j.istr.2011.08.006 ,2011

[22] Dou, W., Chen, Q., Chen, J.," A confidence-based filtering method for DDoS attack defense in cloud environment. Future Generation Computer Systems ", 29, 1838–1850. doi:10.1016/j.future.2012.12.011 , 2013 .

[23] Arockiam L , Parthasarathy G, Monikandan S, "Privacy in cloud computing: a survey " , Computer Science & Information Technology (CS & IT) , DOI : 10.5121/csit.2012.2331, pp. 321–330, 2012.