Security Issues and Challenges in Cloud Computing

Basel Saleh Al-Attab, H. S. Fadewar

Abstract-The cloud computing is a paradigm shift for online services where the cloud computing provides resources, programs and applications as a service via the Internet and according to the user' request. It has the ability to make use of computing resources with minimal costs and at high speed. It can provide users with a range of services, applications, and infrastructure and storage of a large amount of data, including important information. Despite the capabilities of the cloud computing, there is a question mark on its security. Therefore, security has become one of the most important issues in the cloud computing. This paper introduces the concept of the cloud computing, its characteristics and models as well as the various security threats that threaten the cloud computing, It also sheds light on some security issues and challenges in the cloud.

Index Terms: Cloud Computing, Threats, Security Issues, Challenges.

I. INTRODUCTION

Cloud computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes [1]. Cloud computing takes technology, services, and applications that are similar to those on the Internet and turns them into a self-service utility [2]. Security in general, is related to the important aspects of confidentiality, integrity and availability; they thus become building blocks to be used in designing secure systems. These important aspects of security, apply to the three broad categories of assets which are necessary to be secured, data, software and hardware resources [20].

II. CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) defined cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3]. Cloud computing has some characteristics. NIST referred to five essential characteristics: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, and Measured service.

A. Cloud Development Models

There are four main cloud development models that can be shown below:

- *Public Cloud***:** In public cloud, as the name implies, anyone can buy a service from any service provider. The vendor will be taking care of all security concern [5].

  Public clouds are mainly used by small and medium sized company. Here, you have to pay what you have used. Amazon EC2 and Flexi scale are examples of cloud vendors [4].
- *Private Cloud***:** A private cloud is one in which the services and infrastructure are maintained on a private network. Private cloud computing is unlike public cloud, owned and managed privately, and the access can be limited to a single business or a part of it. The private cloud computing is good in terms of security, stability, privacy and data persistence [6]. With private cloud we get the same benefit of public cloud such as self-service, scalability and elasticity and with the additional control and customization available from dedicated resources [5].
- *Hybrid Cloud***:** Hybrid cloud uses resources from both private and public. For example, xyz companies want to host their website in a public cloud but prefer to keep the customer data within its own data center [7].
- *Community Cloud***:** Community cloud is a group of several organizations where they have similar requirements and share the same infrastructure can benefited from cloud computing. Community cloud is more expensive comparing to others but offer high level of privacy, security or policy compliance. Community cloud computing makes use of the principles of Digital Ecosystems to provide a paradigm for clouds in the community, offering an alternative architecture for the use cases of cloud computing [5].

B. Cloud Services Models

Once a cloud computing is established, how its services are deployed in terms of business models can differ depending on requirements. Cloud service delivery is divided among three archetypal models and various derivative combinations [8]. The three fundamental classifications are often referred to as the "SPI Model," where 'S' refers to Software as a service, 'P' to Platform as a service, and 'I' to Infrastructure as a service.

- *Software as a Service***:** SaaS is a complete operating environment with applications, management, and the user interface. In the SaaS model, the application is provided to the client through a thin

Manuscript received on May 18, 2014.

Basel Saleh Al-Attab, Research Scholar, School of Computational Sciences, S. R. T. M. University, Nanded

H.S.Fadewar, Assistant Professor, School of Computational Sciences, S. R. T. M. University, Nanded

client interface (a browser, usually), and the customer's responsibility begins and ends with entering and managing its data and user interaction. Everything from the application down to the infrastructure is the vendor's responsibility [2].

- *Platform as a Service*: PaaS provides virtual machines, operating systems, applications, services, development frameworks, transactions, and control structures. The client can deploy its applications on the cloud infrastructure or use applications that were programmed using languages and tools that are supported by the PaaS service provider. The service provider manages the cloud infrastructure, the operating systems, and the enabling software. Here, the client is responsible for installing and managing the application that it is deploying [2].
- *Infrastructure as a Service*: IaaS provides virtual machines, virtual storage, virtual infrastructure, and other hardware assets as resources that clients can provision. The IaaS service provider manages the entire infrastructure, while the client is responsible for all other aspects of the deployment. This can include the operating system, applications, and user interactions with the system [2].

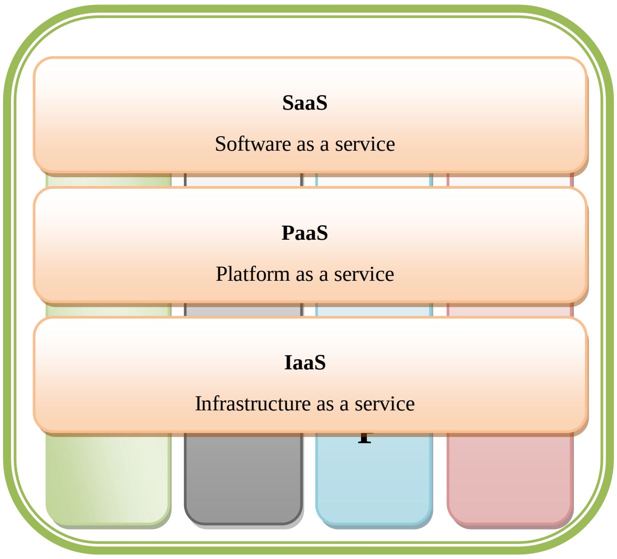

Figure1: Cloud computing models.

C. The Top Nine Threats In Cloud Computing Security

The Cloud Security Alliance (CSA) has identified "The Notorious Nine," the top nine cloud computing threats for 2013. The report reflects the current consensus among industry experts surveyed by CSA, focusing on threats specifically related to the shared, on-demand nature of cloud computing [9]. Samson (2013) explain these threats according to CSA as following [10] :

- *Data Breaches*: The challenge in addressing this threat of data loss and data leakage is that the measures you put in place to mitigate one can exacerbate the other. You could encrypt your data to reduce the impact of a breach, but if you lose your encryption key, you will lose your data. However, if you opt to keep offline backups of your data to reduce data loss, you increase your exposure to data breaches.
- *Data Loss*: Data Loss is the prospect of seeing your valuable data disappears without a trace. A malicious hacker might delete a target's data out of spite -- but then, you could lose your data to a careless cloud service provider or a disaster, such as a fire, flood, or earthquake. Compounding the challenge, encrypting your data to ward off theft can backfire if you lose your encryption key.
- *Account Hijacking*: Cloud computing adds a new threat to this landscape, according to CSA. If an attacker gains access to your credentials, he or she can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or services instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.
- *Insecure APIs*: IT admits rely on interfaces for cloud provisioning, management, orchestration, and monitoring. APIs are integral to security and availability of general cloud services. From there, organizations and third parties are known to build on these interfaces, injecting add-on services. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency.
- *Denial of Service*: DoS outages can cost service providers customers and prove pricey to customers who are billed based on compute cycles and disk space consumed. While an attacker may not succeed in knocking out a service entirely, he or she may still cause it to consume so much processing time that it becomes too expensive for you to run and you will be forced to take it down yourself.
- *Malicious Insiders*: In an improperly designed cloud scenario, a malicious insider can wreak even greater havoc. From Iaas to Paas to SaaS, the malicious insider has increasing levels of access to more critical systems and eventually to data. In situations where a cloud service provider is solely responsible for security, the risk is great. Even if encryption is implemented, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack, according to CSA.
- *Abuse of Cloud Services*: The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes to identify it.
- *Insufficient Due Diligence*: Organizations embrace the cloud without fully understanding the cloud environment and associated risks. CSA's basic advice for organizations is to make sure they have sufficient resources and to perform extensive due diligence before jumping into the cloud.
- *Shared Technology Issues*: Cloud service providers share infrastructure, platforms, and applications to deliver their services in a scalable way. whether it is the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation

properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models.

D. Security Issues in Cloud Computing

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing [11]. Here are some of the important security requirements: Confidentiality, Integrity, Availability, Non-repudiation, Physical security, and Data sanitization [12].Cloud Computing security related issues can be classified into the following five categories as shown in Figure (2):

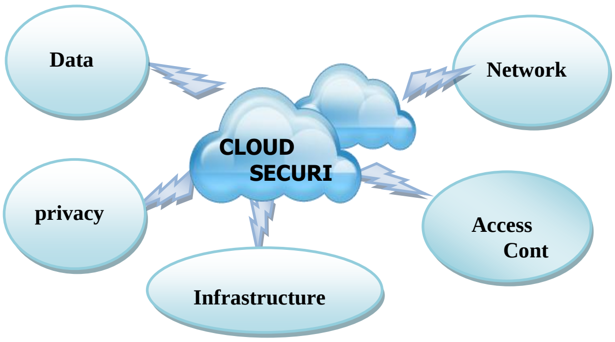

Figure 2: Cloud computing security categories**.**

- *Network security***:** Network has a number of security threats to deal with. To ensure network security the following points, such as confidentiality and integrity in the network, proper access control and maintaining security against the external third party threats should be considered while providing network level security [13]. Network security issues are proper installation of network firewalls, network security configurations, Internet protocol vulnerabilities, and Internet dependence [14].
- *Access Control***:** Access control manages users, files and other resources. It controls user's privileges to files or resources (objects). In access control systems, various steps like, identification, authentication, authorization and accountability are taken before actually accessing the resources or the object in general [15]. Access control issue are account and service hijacking, malicious insiders, authentication mechanism, privileged user access, and browser security.
- *Infrastructure Security***:** The security challenges at various levels namely network level, host level and application level are not specifically caused by cloud computing, instead they are exacerbated by its use [16]. Cloud infrastructure security issues are Insecure interface of API, quality of service, sharing technical flaws, reliability of suppliers, security misconfiguration, multi-tenancy, and server location and backup [14].
- *Data security*: Data security is a significant task, with a lot of complexity. Since the data owner does not know where his/her data is stored and data hosts cannot be considered as completely reliable, data security is the most important concern amongst cloud clients [17]. Because cloud-based services use the Internet, storing data in the cloud can be risky and can mean less control over your data. The following are the data security issues data redundancy, data loss and leakage, data location, data recovery, data privacy, data protection, and data availability.
- *Privacy***:** Cloud model increases the privacy concern because the service provider has access to all the user data that resides in their premises. They may deliberately or accidentally uncover it or misuse the user data. There are some considerations with respect to privacy in cloud including storage, retention, destruction, regulatory compliance, auditing and monitoring and privacy breaches [18]. The following tips are recommended privacy practices for cloud system designers, architects, developers and testers: minimise personal information sent to and stored in the cloud, protect personal information in the cloud, maximise user control, allow user choice, specify and limit the purpose of data usage, and provide feedback [19]. The cloud computing security categories and their related issues are summarized in Table (1):

Table 1: Cloud Computing Security Categories Related Issues

Security Category	**Issues**
Network	- Proper installation of network firewalls. - Network security configurations. - Internet protocol vulnerabilities. - Internet Dependence.
Access Control	- Account and service hijacking. - Malicious insiders. - Authentication mechanism. - Privileged user access. - Browser Security.
Infrastru-cture	- Insecure interface of API. - Quality of service. - Sharing technical flaws. - Reliability of Suppliers. - Security Misconfiguration. - Multi-tenancy. - Server Location and Backup.
Data	- Data redundancy. - Data loss and leakage. - Data location.

	- Data recovery. - Data privacy. - Data protection. - Data availability.
Privacy	- Minimise personal information sent to and stored in the cloud. - Protect personal information in the cloud. - Maximise user control. - Allow user choice. - Specify and limit the purpose of data usage. - Provide feedback.

E. Security Challenges In The Cloud Computing

Securing computer systems have not been an easy task. Cloud computing and cloud service providers need to address a number of challenges that affects security in the cloud [21]. The challenges that need to be addressed are as follows:

- *Loss of governance*: By using cloud services the client passes control to the provider. This passing off, of control to the provider, results in loss of control over a number of issues which in turn may affect the security posture of the client data and applications [21].
- *Malicious insider*: It is usual for a provider to hide his/her own company policy on recruiting employees and what level of access it provides to them, but with higher level of access an employee can gain access to confidential data and services [22].
- *Management interface compromise*: cloud service providers seek to differentiate themselves based upon the controls they offer to users, and the degree to which users can operate controls [23]. As the interface to cloud services is Internet based and allows for remote access to resources by the use of web browser, this increases the risks of malicious activity remotely.
- *Insecure or incomplete data deletion*: What happens when a client requests to delete a cloud resource? Is there possibility of partial deletion? How timely is the deletion made? Given the nature of cloud computing, these questions have no straight answers and in case of hardware re-use the risks are very high to clients [21].
- *Data interception*: Given the distributed nature of cloud computing architecture, the amount of data in transit is increased greatly as opposed to conventional computing environment. This makes cloud computing more susceptible to attacks such as: replay attacks, man-in-the-middle attacks, sniffing and spoofing [21].

Moreover there are other challenges that may impact cloud computing security though they may not be directly related to it. These challenges are such as: network breaks, modification of network traffic, management issues of cloud resources such as congestion, misconnection, and non-optimal use of resources.

III. CONCLUSION

In brief, the most important goal of the cloud is to provide high-performance cloud computing for customers with a low cost without relying on the infrastructure of their own. Despite the security threats that are mentioned in the cloud computing are present in the traditional computing model, they are more influential in the cloud computing. There are many researches conducted with reference to security issues of the cloud computing. These researches have proposed several methods and monitoring tools to eliminate security threats in the cloud and provided an integrated security framework to solve the security issues at different levels.

REFERENCE

1. Sabahi, F," Cloud computing security threats and responses", Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on 27-29 May 2011.
2. Barrie Sosinsky,"cloud computing bible", Copyright © 2011 by Wiley Publishing, Inc., Indianapolis, Indiana
3. Peter Mell and Tim Grance, " The NIST Definition of Cloud Computing", Version 15, 10-7-09 ,National Institute of Standards and Technology, Information Technology Laboratory
4. http://en.wikipedia.org/wiki/Cloud_computing
5. Ajith Singh. N,Vasanthi.V , M. Hemalatha, " A Brief Survey on Architecture, Challenges & Security Benefit in Cloud Computing", Volume 2 No. 2, February 2012 ISSN 2223-4985 International Journal of Information and Communication Technology Research, ©2012 ICT Journal. All rights reserved
6. Y. Ghebghoub, S. Oukid, and O. Boussaid," A Survey on Security Issues and the Existing Solutions in Cloud Computing", International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013
7. http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud.
8. Introduction to cloud computing www.dialogic.com/~/media/products/docs/whitepapers /12023-cloud-computing- wp.pdf
9. CSA Cloud Security Alliance,Top Threats working Group, The Notorious Nine cloud computing top threats in 2013
10. Ted Samson ," 9 top threats to cloud computing security", February 25, 2013, http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428
11. Kevin Hamlen, Murat Kantarcioglu," Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010 .
12. Ali Asghary Karahroudy," Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System",July, 2011
13. Rohit Bhadauria, Rituparna Chaki," A Survey on Security Issues in Cloud Computing",http://www.tifr.res.in/~sanyal/papers/Survey_on_Security_Issues_in_Cloud_Computing_and_Associated_Mitigation_Techniques.pdf
14. Issa M. Khalil 1,*, Abdallah Khreishah 2 and Muhammad Azeem 3," Cloud Computing Security: A Survey", Computers 2014, 3, 1-35; doi:10.3390/computers3010001
15. Abdul Raouf Khan," ACCESS CONTROL IN CLOUD COMPUTING NVIRONMENT", VOL. 7, NO. 5, MAY 2012 ISSN 1819-6608 ARPN Journal of Engineering and Applied Sciences
16. Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks and Compliance, O'Reilly Media, Inc., 2009.
17. Savita Bhayal," A STUDY OF SECURITY IN CLOUD COMPUTING ", August 2011

18. S.SUDHA1, V.MADHU VISWANATHAM2," ADDRESSING SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING", Journal of Theoretical and Applied Information Technology 20th February 2013. Vol. 48 No.2 © 2005 - 2013 JATIT & LLS. All rights reserved.
19. Siani Pearson," Taking Account of Privacy when Designing Cloud Computing Services", HP Laboratories HPL-2009-54
20. Dimitrios Zissis , Dimitrios Lekkas," Addressing cloud computing security issues", Future Generation Computer Systems 28 (2012) 583–592
21. Faith Shimba, "Cloud Computing:Strategies for Cloud Computing Adoption",Dublin Institute of Technology ARROW@DIT, 2010-09-01
22. Md. Tanzim Khorshed, A.B.M. Shawkat Ali , Saleh A. Wasimi," A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing",Future Generation Computer Systems 28 (2012) 833–851.
23. Sadie Creese and Paul Hopkins,"Global Security Challenges of Cloud Computing", International Digital Laboratory, WMG, University of Warwick, UK, Draft v0.7 – July 27