Seven Deadly Threats and Vulnerabilities in Cloud Computing

Mervat Adib Bamiah
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
mervatbamiah@yahoo.com

Sarfraz Nawaz Brohi
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
sarfraz_brohi@hotmail.com

Abstract— **Cloud computing has been developed to reduce IT expenses and to provide agile IT services to individual users as well as organizations. It moves computing and data away from desktop and portable PCs into large data centers. This technology gives the opportunity for more innovation in lightweight smart devices and it forms an innovative method of performing business. Cloud computing depends on the internet as a medium for users to access the required services at any time on pay-per-use pattern. However this technology is still in its initial stages of development, as it suffers from threats and vulnerabilities that prevent the users from trusting it. Various malicious activities from illegal users have threatened this technology such as data misuse, inflexible access control and limited monitoring. The occurrence of these threats may result into damaging or illegal access of critical and confidential data of users. This research paper describes the characteristics (threats, vulnerabilities) associated with a stormy cloud.**

Keywords- Illegal access, Threats, Vulnerabilities

I. INTRODUCTION

The traditional era of computing involves the use of software, hardware and storage to achieve the required computational service whereas cloud computing has isolated the services from resources (networks, storage, servers). The required services are provided to the users by utilizing the resources of provider. Users are no longer required to purchase hardware, software or to manage storages. Due the evolution of this technology users are required to pay for cloud services on consumption basis. New cloud based business models are being discussed, defined, and implemented as solutions in form of on-demand services that allows businesses to enhance their efficiency and scalability. Success or failure of this technology relies on users' trust whether the service provided is reliable, available and secure. Considering the benefits of cloud computing various organizations are moving towards IT solutions that are based on cloud however, before starting the journey to cloud, organizations must considers the possible threats and vulnerabilities that may convert their dreams of enhancing scalability and saving management cost into a nightmare of data loss and misuse. The users must consider that cloud can be rainy as well, in other words this technology is not trustworthy as it is affected with threats and vulnerabilities. We have termed a cloud with threats and vulnerabilities as a stormy cloud. Based on Cloud Security Alliance (CSA) and our research, we have identified top seven threats and vulnerabilities that are the causes behind the creation of a stormy cloud [1]. The identified threats and vulnerabilities are ranked from top to bottom as shown in Fig.1.

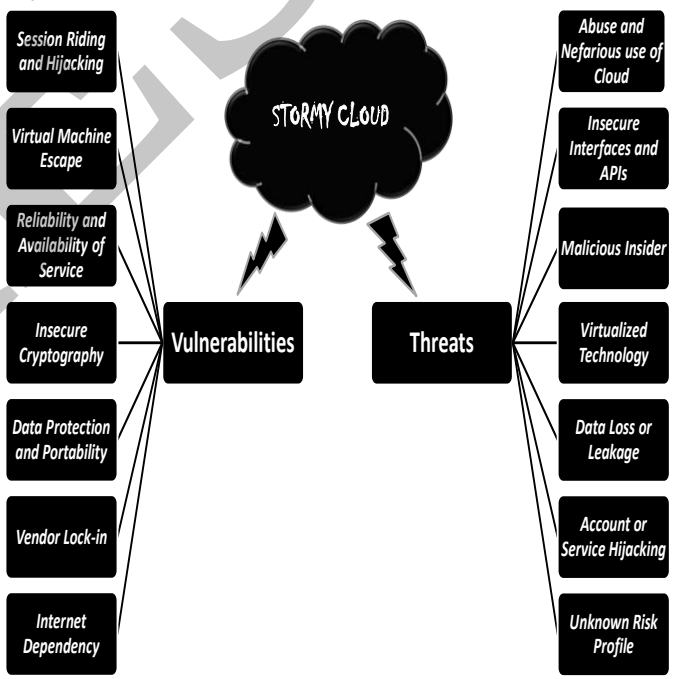

Figure 1. Characteristics of stormy cloud.

In order to create awareness and protect the cloud users from adopting a stormy cloud, we are describing the impacts of threats and vulnerabilities in cloud computing so that organizations or users can adopt this technology with trust and from a trusted provider who has the powerful and trusted security polices as well as efficient techniques for securing the users' data on cloud.

II. CLOUD COMPUTING THREATS

As we already mentioned, there are several significant threats that should be considered before adopting the paradigm of cloud computing, these threats are discribed as follows :

A. Abuse and Nefarious Use of Cloud

Cloud providers facilitate the users with various types of services including unlimited bandwidth and storage capacity. Some cloud service providers offer free limited trial periods that gives an opportunity for hackers to access the cloud immorally, their impact includes decoding and cracking of passwords, launching potential attack points and executing malicious commands. Spammers, malicious code authors and other cybercriminals can conduct their activities with relative impunity, as cloud service providers are targeted for their weak registration systems and limited fraud detection capabilities. For example some cybercriminals use rich content applications such as flash files that enable them to hide their malicious code and utilize users' browsers to install malware [1].

B. Insecure Interfaces and APIs

Cloud users are using software interfaces and APIs to access and manage the cloud services. These APIs need to be secured because they play an integral part during provisioning, management, orchestration and monitoring of the processes running in a cloud environment. The security and availability of cloud services is dependent upon the security of these APIs so they should include features of authentication, access control, encryption and activity monitoring. APIs must be designed to protect against both accidental and malicious attempts to avoid threats. If cloud service provider relies on weak set of APIs, variety of security issues will be raised related to confidentiality, integrity, availability and accountability such as malicious or unidentified access, API dependencies, limited monitoring/logging capabilities, inflexible access controls, anonymous access, reusable tokens/passwords and improper authorizations[1].

C. Malicious Insider

Insider attacks can be performed by malicious employees at the provider's or user's site. Malicious insider can steal the confidential data of cloud users. This threat can break the trust of cloud users on provider. A malicious insider can easily obtain passwords, cryptographic keys and files. These attacks may involve various types of fraud, damage or theft of information and misuse of IT resources. The threat of malicious attacks has increased due to lack of transparency in cloud provider's processes and procedures [2]. It means that a provider may not reveal how employees are granted access and how this access is monitored or how reports as well as policy compliances are analyzed. Additionally, users have little visibility about the hiring practices of their provider that could open the door for an adversary, hackers or other cloud intruders to steal confidential information or to take control over the cloud. The level of access granted could enable attackers to collect confidential data or to gain complete control over the cloud services with little or no risk of detection. Malicious insider attacks can damage the financial value as well as brand reputation of an organization.

D. Virtualized Technology

Due to the cloud virtualization, cloud providers are residing the user's applications on virtual machines (VMs) within a shared infrastructure. The VMs are virtualized based on the physical hardware of cloud provider. In order to maintain the security of users, providers are isolating the VMs from each other so if any of them is malicious, it will not affect the other VMs under the same provider. The VMs are managed by hypervisor in order to provide virtual memory as well as CPU scheduling policies to VMs. As the hypervisor is main source of managing a virtualized cloud platform, hackers are targeting it to access the VMs and the physical hardware, because hypervisor resides between VMs and hardware [3], so attack on hypervisor can damage the VMs and hardware. Strong isolation should be employed to ensure that VMs are not able to impact or access the operations of other users running under the same cloud service provider. Several vendors such as Xen and KVM are providing strong security mechanisms of securing the cloud hypervisors, but still it is identified that sometimes security of VMs is compromised.

E. Data Loss or Leakage

Data loss can occur due to operational failures, unreliable data storage and inconsistent use of encryption keys. Operational failure refers to deletion or alteration of records without a backup of the original content that can take place intentionally or unintentionally. Unreliable data storage refers to saving of data on unreliable media that will be unrecoverable if data is lost [4]. The inconsistent use of encryption keys will result into loss and unauthorized accesses of data by illegal users that will lead to the destruction of sensitive and confidential information. Example of data loss is Twitter hacks. The online accounts of Twitter accessed by hackers and their numerous sensitive corporate documents were stolen. These documents were housed in Google's online web office service Google Docs. Although Google was not the one to be blamed for security break-in as the security of documents from twitter was not efficient enough. Instead, the entire company data was only one password crack away from discovery [5]. It's clear from this example that data loss or leakage can damage one's brand, reputation and cause a loss that may significantly impact employee, partner and users' morale as well as trust. Loss of core intellectual property can have competitive and financial implications beside the compliance violations and legal consequences.

F. Account or Service Hijacking

Account or service hijacking refers to unauthorized access gained by attackers to control the users' accounts, such as phishing, fraud and exploitation of software vulnerabilities. For example if an attacker gains access to users' credentials, they can spy on their activities/transactions, manipulate their data, return falsified information and redirect them to illegitimate sites [6]. Users' account or service instances may become a new base for the attackers who can leverage the

cloud service providers' reputation by launching subsequent attacks. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Authentication and authorization through the use of roles and password protecting is a common way to maintain access control when using web-browsers to access cloud computing systems. However, this method is not sufficient enough to secure sensitive and critical data.

G. *Unknown Risk Profile*

It is important for the users to know software versions, security practices, code updates and intrusion attempts. While adopting cloud computing services, these features and functionality may be well advertised but what about the details or compliance of the internal security procedures, configuration hardening, patching, auditing and logging. Users must be clarified how and where their data and related logs are stored. However, there is no clear answer that leaves users with an unknown risk profile that may include serious threats [1].

III. CLOUD COMPUTING VULNERABILITIES

There are several significant vulnerabilities that should be considered when an organization is ready to move their critical applications and data to a cloud compuitng environment, these vulnerabilities are discribed as follows :

A. *Session Riding and Hijacking*

Session hijacking refers to use of a valid session key to gain unauthorized access for the information or services residing on a computer system, it also refers to theft of a cookie used to authenticate a user to a remote server and it is relevant to web application technologies weaknesses in the web application structure at their disposal that gives the chance to hackers in order to accomplish a wide variety of malicious activities. While session riding refers to the hackers sending commands to a web application on behalf of the targeted user by just sending that user an email or tricking the user into visiting a specially crafted website. Session riding deletes user data, executes online transactions like bids or orders, sends spam to an intranet system via internet and changes system as well as network configurations or even opens the firewall [12]. However, the web technologies evolution and refinement also brings new techniques that compromise sensitive data, provide access to theoretically secure networks and pose threats to the daily operation of online businesses.

B. *Virtual Machine Escape*

Cloud computing servers use the same OS, enterprise and web applications as localized VMs and physical servers. The ability for an attacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments [7]. In addition, co-location of multiple VMs increases the attack surface and risk of VM-to-VM compromise. Intrusion detection and prevention systems need to be able to detect malicious activity at VM level, regardless of the location of the VM within the virtualized cloud environment.VM escape is a vulnerability that enables a guest-level VM to attack its host. Under this vulnerability an attacker runs code on a VM that allows an OS running within it to break out and interact directly with the hypervisor as shown in Fig.2 [8].

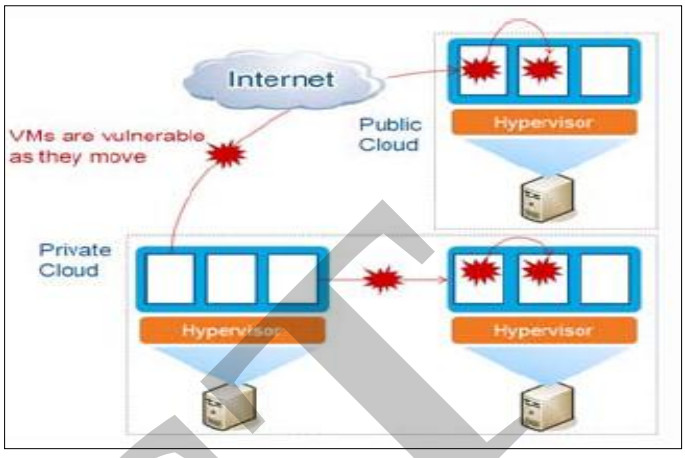

Figure 2. VM Escape.

It allows the attacker to access the host OS and all other VMs running on that particular host. Hypervisors and VM's complexity may cause an increase threat to attack surface that weakens security such as paging, check pointing and migration of VMs [8].

C. *Reliability and Availability of Service*

In terms of reliability and availability, cloud computing is not a perfect technology. For-example in February 2008, Amazon's Web Service (Amazons-S3) cloud storage infrastructure went down for several hours, causing data loss and access issues with multiple Web 2.0 services. With more services being built on top of cloud computing infrastructures, an outage or failure can create a domino effect by taking down large amounts of Internet based services and applications which raise several questions such as in cases of failure, what forms of settlement exist for stakeholders? What is the responsibility of cloud providers? What will be appropriate procedures to overcome these issues? [9].

D. *Insecure Cryptography*

Attackers' can decode any cryptographic mechanism or algorithm as main methods to hack them are discovered. It's common to find crucial flaws in cryptographic algorithm implementations, which can twist strong encryption into weak encryption or sometimes no encryption at all. For example in cloud virtualization providers uses virtualization software to partition servers into images that are provided to the users as on-demand services [10]. Although utilization of those VMs into cloud providers' data centres provides more flexible and efficient setup than traditional servers but they don't have enough access to generate random numbers needed to properly encrypt data. This is one of the fundamental problems of cryptography. How do computers produce truly random numbers that can't be guessed or replicated? In PCs, OS

typically monitors users' mouse movements and key strokes to gather random bits of data that are collected in a so-called Entropy Pool (a set of unpredictable numbers that encryption software automatically pulls to generate random encryption passkeys). In servers, one that don't have access to a keyboard or mouse, random numbers are also pulled from the unpredictable movements of the computer's hard drive. VMs that act as physical machines but are simulated with software have fewer sources of entropy. For example Linux-based VMs, gather random numbers only from the exact millisecond time on their internal clocks and that is not enough to generate strong keys for encryption [11].

E. Data Protection and Portability

Although the cloud services are offered based on a contract among client and a provider but what will happen when the contract is terminated and client doesn't wants to continue anymore. The question is, will the sensitive data of client be deleted or misused by the provider. Secondly if the provider went out of business due to any reason, what will happen to the services and data of the client? Will the provider handout the data of client to some other provider, if yes, will client trust the new provider? Considering these questions we can say that data protection and portability remains as one of main weaknesses of cloud computing.

F. Vendor Lock-in

This vulnerability occurs due to immature providers and new business models which raise the risk of failure and going out of the business. Lock-in, makes a client dependent on a provider for products and services so they will be unable to deal with another provider without substantial switching costs. Clients must be sure of their potential provider prior to provider selection process. Lack of standards may also lock-in the clients with only one provider. Due to heterogeneous standards and policies settled by each provider, clients are not able to easily migrate from one provider to another even though they want to do so [13].

G. Internet Dependency

Cloud computing is an internet dependent technology where users are accessing the services via web browser. What if internet is not available or service is down, what will happen to users systems and operations that are very critical and need to run 24 hours such as Healthcare and Banking systems. In some Asian and African underdeveloped countries where service of internet is not considered as reliable enough, will organizations adopt this paradigm to move their significant systems on cloud?

IV. Conclusion and Future Work

In this research paper we have discussed the characteristics of a stormy cloud that contains threats and vulnerabilities. Cloud computing has a dynamic nature that is flexible, scalable and multi-shared with high capacity that gives an innovative shape of carrying out business [14]. However, beside these benefits there are seven deadly threats and vulnerabilities encountered in this technology. Therefore, we believe there is still tremendous opportunity for researchers to make revolutionary contributions in this field and bring significant impact of their development to the industry. There is need to develop and design in-depth security techniques and policies in terms of people, processes and technology. By considering the contributions from several IT industries worldwide, it's obvious that cloud computing will be one of the leading strategic and innovative technologies in the near future.

Acknowledgment

The glory of accomplishing this research paper goes to our parents for their moral support. We are also thankful to our supervisor for encouraging us to write this research journal. Finally, we are thankful to IJAEST for assisting us to review this journal and providing us timely response.

References

[1] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" Cloud Security Alliance, 2009, [Online], Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, [Accessed: 08-July-2011].

[2] E., Mathisen, "Security challenges and solutions in cloud computing," in Digital Ecosystems and Technologies Conference (DEST), 2011 *Proceedings of the 5th IEEE International Conference on*, 2011, pp. 208-212.

[3] Wei Chen, Hongyi Lu, Li Shen, Zhiying Wang, Nong Xiao, and Dan Chen, "A Novel Hardware Assisted Full Virtualization Technique," in *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*, 2008, pp. 1292-1297.

[4] S. Farrell, "Portable Storage and Data Loss," *Internet Computing, IEEE*, vol. 12, no. 3, pp. 90-93, 2008.

[5] R., Trope, C., Ray, "The Real Realities of Cloud Computing: Ethical Issues for Lawyers, Law Firms, and Judges ", [Online], Available: http://ftp.documation.com/references/ABA10a/PDfs/3_1.pdf , 2009, [Accessed: 15-Jul-2011].

[6] Karthick Ramachandran, Thomas Margoni and Mark Perry, "Clarifying Privacy in the Clouds" in *CYBERLAWS 2011 : The Second International Conference on Technical and Legal Aspects of the e-Society, IARIA,2011*.

[7] S., Subashini, V. Kavitha. "A survey on security issues in service delivery models of cloud computing". *Journal of Network and Computer Applications*, vol.34, pp.1-11, 2011.

[8] Trend Micro, "Making Virtual Machines Cloud-Ready", [Online], Available: http://www.whitestratus.com/docs/making-vms-cloud ready.pdf. *A Trend Micro White Paper*, 2009 [Accessed: 16-Jul-2011].

[9] J., Grimes, P., Jaeger, J., Lin, "Weathering the Storm: The Policy Implications of Cloud Computing" [Online], Availablehttp://ischools.org/images/iConferences/CloudAbstract13109FINAL.pdf , [Accessed: 19-Jul-2011].

[10] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE, vol. 9, no. 2, pp. 50-57, 2011.

[11] A., Greenberg, "Why Cloud Computing Needs More Chaos" [Online], Available:http://www.forbes.com/2009/07/30/cloud-computing-security-technology-cio-network-cloud-computing.html, 2009, [Accessed: 20-Jul-2011].

[12] T. Schreiber, "Session Riding a Widespread Vulnerability in Today's Web Applications" [Online], Available: http://www.securenet.de/papers/Session_Riding.pdf, white paper, 2004. [Accessed: 20-Jul-2011].

[13] G., Petri, "Vendor Lock-in and Cloud computing", [Online], Available: http://cloudcomputing.sys-con.com/node/1465147 , 2010, [Accessed: 23-Jul-2011].

[14] S., Brohi, M., Bamiah, "Challenges and Benefits for Adopting the Paradigm of Cloud Computing", *International Journal of Advanced Engineering Sciences and Technologies* (IJAEST), vol. 8, pp. 286 - 290, 2011.

