IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-6, Issue-3 E-ISSN: 2347-2693

Threats and Vulnerabilities of Cloud Computing: A Review

P.S. Suryateja

CSE Dept., Vishnu Institute of Technology, Bhimavaram, India

Available online at: www.ijcseonline.org

Received: 19/Feb//2018, Revised: 25/Feb2018, Accepted: 17/Mar/2018, Published: 30/Mar/2018

***Abstract* —** Cloud computing is a new frontier in computing technologies. It is well known for its pay-per-use model for billing customers and providing other features like elasticity, ubiquity, scalability, and availability of resources for businesses. Cloud computing provides delivery models like Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) which can be utilized by various organizations to solve their data storage and processing needs. From recent surveys conducted by well known reputed cloud providers, it is apparent that more and more organizations and enterprises are moving their workloads to cloud. The top concern among the organizations to move their workloads or processes to cloud is security. Even though the security measures provided in cloud computing are evolving over the years, it still remains as a major challenge or obstacle. This paper provides an overview of numerous threats and vulnerabilities of cloud computing which can act as a guide to decision makers in organizations to evaluate the security in clouds.

***Keywords*—**Cloud Computing, Cloud Security, Cloud Threats, Cloud Vulnerabilities

I. INTRODUCTION

In the recent years, adoption of cloud computing is increasing at an unprecedented pace [12]. There is a steady increase in the number of organizations moving their workloads to cloud. A lot of research is being conducted both by academicians and industry [1] to standardize the challenges posed by cloud computing like VM allocation, power conservation, improving security, etc.

Cloud computing can be defined in many ways. There is no universal definition for it. NIST's (National Institute of Standards and Technology) definition of cloud computing is considered as the de facto definition. NIST defines cloud computing as "cloud computing is a model for enabling ubiquitous, 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."

The essential characteristics of cloud computing are as follows:

On-demand self-service: The resources are provisioned as per user demand and it must be done with little or no service provider intervention.

Broad network access: Resource or services must be accessible anywhere through thin or thick clients (Ex: PCs, laptops, mobile phones, etc.) via the internet.

Resource pooling: Providers pool several resources and provide them to users using a multi-tenant model. This result in economies of scale.

Rapid elasticity: Resources must be scaled in and out based on user demand. This elastic provisioning should be done automatically.

Measured service: Resource or service usage is monitored, controlled and reported providing transparency for both the provider and consumer of the service. The consumer pays only for what he/she uses (pay-per-use model).

Cloud delivery models as shown in Figure 1, allow consumers to access the services provided by cloud service providers. These are discussed in detail below:

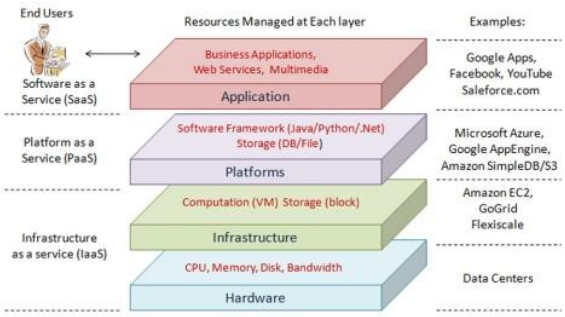

Figure 1: Cloud delivery models and architecture

Software-as-a-Service (SaaS): In this model the consumers can use the application services provided by the cloud providers. The consumers can access the service through thin clients (Ex: web browsers) or through APIs. Consumers have no control over the application or the underlying operating system and infrastructure. The only control provided to the consumer is changing the user configuration settings. Examples of SaaS providers include Google Apps, Facebook, YouTube, Salesforce, etc.

Platform-as-a-Service (PaaS): In this model consumers can develop or deploy their own applications on the platform (languages, libraries, and tools) provided by the cloud provider. Consumers have no control over the underlying operating system and infrastructure (servers, storage, network, etc.). Consumers will have limited control to modify the environment (platform) settings. Examples of PaaS providers include Microsoft Azure, Google AppEngine, IBM Bluemix, Amazon Simple DB/S3, etc.

Infrastructure-as-a-Service (IaaS): In this model consumer is able to provision processing, storage, network and other resources on which the consumer can develop or deploy an application. The consumer can't manage the underlying cloud infrastructure but has control over the operating system, firewall, storage and deployed applications. Examples of IaaS providers include Amazon EC2, GoGrid, Flexiscale, etc.

Apart from the features and services provided by cloud computing, there are several issues that act as a hindrance to its adoption [8,10]. Based on the survey conducted by a leading SaaS provider, RightScale, one of the major challenge in the adoption of cloud computing is security as shown in Figure 2.

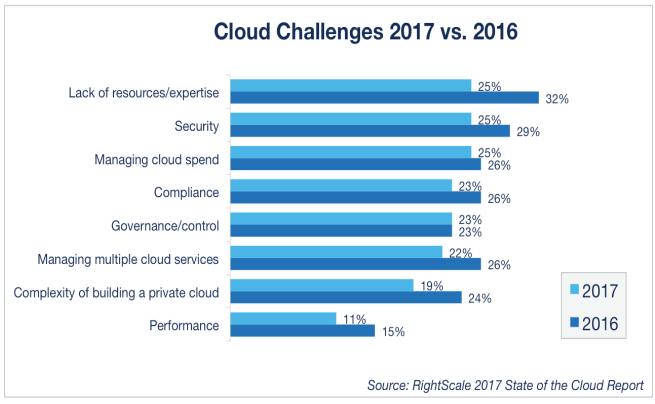

Figure 2: Cloud challenges 2017 vs. 2016

An exhaustive search for various threats and the vulnerabilities related to those threats was performed and an overview of those is presented in this paper. The goal of a Chief Information Security Officer (CISO) and his/her team is to minimize the threats by providing countermeasures to various vulnerabilities that affect the security of the organization or enterprise. This paper provides a baseline for various threats and vulnerabilities in cloud computing.

The novel addition in this research is the inclusion of latest threats like Ransomware and Spectre and Meltdown which are unfound in the literature. In the past few years, the most troublesome malware infecting the cloud was Ransomware, which almost encrypts everything and makes the assets inaccessible. Spectre and Meltdown are the most recent threats which arise because of vulnerabilities in cloud hardware and are common across all the hardware manufacturers. Although patches for these vulnerabilities are being released, it is not easy to utilize them. These are significant threats that need to addressed by every cloud service provider and customer.

Entire information in this paper is organized as follows: Section I provides an introduction to cloud computing and the need for giving importance to the security in cloud computing. Section II provides an overview of threats and vulnerabilities of cloud computing and finally Section III concludes with the future scope of the research.

II. THREATS AND VULNERABILITIES

A threat is a potential cause of an incident that may result in harm to a system or an organization. A vulnerability is a weakness in the asset or system which is exploited by a threat. A threat agent carries out threats by exploiting one or more vulnerabilities. By conducting an exhaustive literature survey, various threats and vulnerabilities for cloud computing are identified. They are discussed in detail below:

Data Breaches (T01): A data breach is a security incident in which sensitive, private, or confidential data related to a person or organization has been accessed, copied, or transmitted by an unauthorized party. Data breach is a threat with severe risk and is ranked as number one [4,9] among the threats in cloud computing. Over 1.4 billion records were lost to data breaches in 2017 alone, many of which involved cloud servers. Equifax breach [3] affected at least 143 million people. OneLogin, which provides identity management and single sign-on capabilities for cloud services was hacked in May 2017. Data breaches can be caused due to targeted attacks, simple human error, application vulnerabilities, or poor security practices.

Data Loss (T02): It is corruption or unavailability of data which results due to natural disasters [3] like floods, earthquakes; and simple human errors like when a cloud administrator accidentally deletes files, hard drive failure, power failure, or due to malware infection. To avoid data loss, the most efficient strategy is to backup data to multiple

locations so that even when data gets corrupted or lost at one location, it can be replaced with a copy available at another location.

Malicious Insiders (T03): Perhaps the most devastating threat with highest risk is a malicious insider. An insider threat can take different forms [5] like a former employee, system administrator, third-party contractor, or a business partner. An insider threat can be disastrous. As an example, a recent insider breach in Sage, resulted in the company's stock price dropping by 4.3%, causing millions of dollars in losses. Systems that depend solely on cloud service providers for security are at a more excessive risk. A malicious insider such as a system administrator can access potentially confidential information and can acquire increasing levels of access to more critical systems and eventually may cause a data breach.

Denial of Service (T04): A DoS (Denial of Service) attack as shown in Figure 3, effects the availability of a system. In a DoS attack, there is only one source machine from which the attack originates and it is susceptible to mitigate. DoS attacks are designed to prevent legitimate users of a service from being able to access their data or applications.

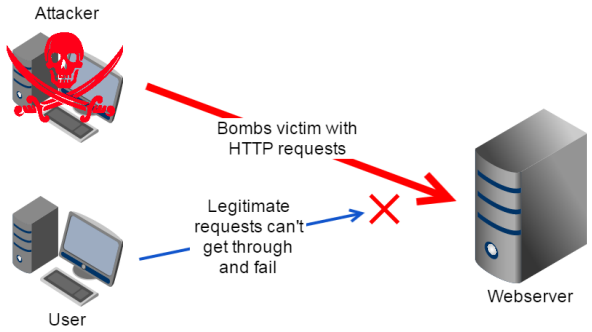

Figure 3: Denial of Service (DoS) attack

A DDoS (Distributed Denial of Service) attack as shown in Figure 4 on the other hand, employs several systems to attack a cloud service. In a DDoS attack, the attacker takes control of several victim systems known as zombies or slaves by spreading different kinds of malware. This collection of slaves is known as a botnet. Now, the attacker can take down a cloud service by ordering the slaves in the botnet to send fake traffic which fabricates data or applications or other resources in cloud unavailable to legitimate users.

Both DoS and DDoS attacks are easy to execute, especially if the attacker has control over a botnet. Now-a-days, these services are available online for a modest fee and there is no need to make your own botnet. One high-profile example of DDoS [6] occurred in October 2016, when an attack on Internet DNS (Domain Name Service) company, Dyn, brought down many major websites throughout the U.S. and Europe. A variation of DoS or DDoS, particularly related to cloud is Economic Denial of Sustainability (EDoS) attack [11], where an attacker sends fake requests to a victim cloud service to have an economic affect.

Vulnerable Systems and APIs (T05): Cloud APIs (Application Programming Interfaces) represent an open door for public to your cloud application. Exploiting a cloud API can grant an attacker considerable access to cloud resources. Cloud Service Providers (CSP) exposes a set of software user interfaces or APIs that customers use to interact with cloud services. Those APIs should be designed to protect against accidental and malicious attempts.

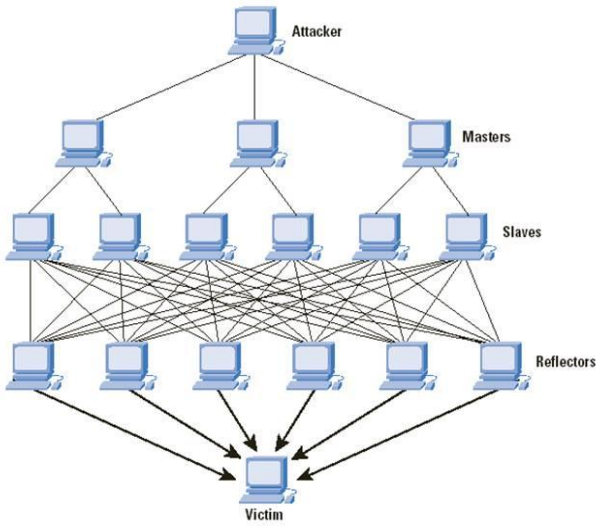

Figure 4: Distributed Denial of Service (DDoS) attack

The underlying Operating System (OS) at the PaaS level may contain vulnerabilities which are exploitable bugs in system programs that allow the attacker to gain control of the system or disrupt the service operations. Also, a hypervisor at the IaaS level, might contain vulnerabilities which can be exploited to breach the confidentiality, integrity and availability of all the tenants (customers) on a single or multiple machines. A 2017 report by RedLock found that 40% of organizations using cloud storage services had inadvertently exposed one or more services to the public. For more considerable security, cloud APIs should be accessed via encrypted keys [13], which are used to authenticate the API user.

Weak Authentication and Identity Management (T06): Organizations or enterprises often encounter difficulty with identity management as they try to allocate appropriate permissions to every user's job role. The Anthem Inc data breach resulted in cyber criminals accessing 80 million

records of personal and medical information. This attack was the result of stolen user credentials. Attackers masquerading as legitimate users, operators or developers can access and modify data, issue control plane and management functions, sniff data in transit, or inject malicious software that appears to originate from a legitimate source [4].

Account Hijacking (T07): Cloud services add a new threat to the landscape of account or service hijacking. Account hijacking is compromising the account credentials of a legitimate user and utilizing them for nefarious purposes. With stolen credentials, attackers might compromise the confidentiality, integrity, or availability of the cloud services. Techniques like phishing and fraud allow attackers to hijack account credentials. Enterprises should mitigate the sharing of account credentials between users and cloud services and enable multifactor authentication where ever possible.

Shared Technology Vulnerabilities (T08): Cloud computing provides multi-tenancy where multiple users share different cloud resources. Underlying components that comprise the infrastructure supporting cloud services deployment may not have been designed to offer strong isolation properties for a multi-tenant architecture or multi-customer applications. This can lead to shared technology vulnerabilities related to Virtual Machines (VMs), operating systems, hypervisor, etc. A vulnerability or misconfiguration in a shared platform component can allow an attacker to compromise the cloud data security of many or all customers, resulting in a data breach. Best practices around client implementation and data management help protect against shared technology vulnerabilities.

Lacking Due Diligence (T09): Due diligence is the process of evaluating CSPs to ensure that best practices are in place. A part of this process includes verifying whether the cloud provider can offer necessary security controls and meet the level of service expected by the customer. Enterprises should review accreditations and standards gained by CSPs including ISO 9001, DCS, PCI, and HIPAA. Lack of due diligence massively affects application security resulting in breach.

Advanced Persistent Threats (T10): An Advanced Persistent Threat (APT) is a type of attack in which the attacker infiltrates systems to establish a foothold in the infrastructure of an organization in the cloud, from which they steal data. APTs purse their targets stealthily over extended periods of time, often adapting to the security measures intended to defend against them. These types of attacks are very hard to detect as they evolve their defenses. APTs get into cloud services through techniques like spear phishing, direct hacking, attack code on USB devices, penetration through the network and the use of unsecured third-party APIs. Advanced security controls, frequent infrastructure monitoring, and rigid process management are key to defending against this threat to cloud infrastructure.

Abuse of Cloud Services (T11): Poorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups via payment interfaces expose cloud computing models to malicious attacks. Examples of abuse of cloud-based resources include launching DDoS or EDoS attacks, email spam, and phishing campaigns.

A Lack of Responsibility (T12): Often cloud service customers think that the security is sole responsibility of the CSP and often neglect safeguarding their applications in the cloud. Cloud providers have no obligation to protect customer workloads or data beyond the services agreed upon in the Service Level Agreement (SLA) [7].

Insufficient Security Tools (T13): Public providers have an array of tools, and services designed to improve cloud security, verify the state of cloud resources and mitigate attacks. It can be almost inadmissible for cloud users to deal with certain attacks, such as DDoS in progress.

Human Error (T14): Even in this age of computing, the human element is still one of the weakest links in IT security. In the cloud, the risk of human error multiplies because compromised credentials can wreak havoc across applications and data. Phishing, fraud and other forms of social engineering allows hackers to steal credentials and thereby hijack cloud accounts. Administrators should offer security education, and certifications to users, write, clear, acceptable use policies and apply other security best practices.

Ransomware (T15): A type of malware using which an attacker locks files or other resources in the victim's system generally through encryption is called ransomware. To decrypt the files, the attacker requires a ransom. There is no guarantee that the attacker will send the key to decrypt files even when the ransom is paid. In 2017, WannaCry ransomware crippled data at companies and government agencies worldwide [6]. According to the FBI, there were 4000 ransomware attacks per day in 2016, a 300% increase over the previous year. Ransomware can come from multiple sources like email, video, PDF file or a website link, a connected device, or even by a password hack. Ransomware encrypts everything that is attached to a system. In order to be safe, backups should be always saved in different cloud location.

Spectre and Meltdown (T16): These are the names given to latest (2018) set of vulnerabilities in the underlying hardware that affects nearly every computer chip manufactured by all the vendors in the last 20 years. They allow attackers to access data that was previously deemed to be safe. Both Spectre and Meltdown allow side-channel attacks because

they break down the isolation between applications. An attacker that is able to access a system through unprivileged log-in can comprehend information from the kernel, or attackers can read the host kernel if they are a root user on a guest VM. This is a critical issue for all CSPs. While patches are being available, they can only make it harder to execute an attack. Also, the patches might decrease the overall system performance.

Unprotected IoT Devices (T17): A communication technology bringing in traction over the past few years is Internet of Things (IoT). IoT devices require heavy automation for setup, configuration, and patching [7]. A single error could multiply many folds through the use of automated IoT management tools and generate millions of new attack vectors. The network plays a vital role in IoT. All the IoT devices must have strong network security. Additionally, periodic audits should be conducted to examine the setup and management of IoT devices to make sure they maintain the most secure device posture.

III. CONCLUSION AND FUTURE SCOPE

Cloud computing security is a new type of computing model which many organizations are trying to adopt due to its inherent advantages. Security in cloud computing is still evolving, new threats and vulnerabilities are being uncovered. Due to this, the adoption of cloud computing for business processes is slowing down. This paper presents an overview of threats and vulnerabilities of cloud computing. An overview of threats like data breaches, data loss, malicious insiders, denial of service, vulnerable systems and APIs, weak authentication and identity management, account hijacking, shared technology vulnerabilities, lacking due diligence, advanced persistent threats, abuse of cloud services, a lack of responsibility, insufficient security tools, human error, ransomware, Spectre and Meltdown, unprotected IoT devices and the associated vulnerabilities for each of these threats is present in Table 1 below.

Table 1. Threats and Vulnerabilities of Cloud Computing

Threat No.	Threat Name	Possible Vulnerabilities
T01	Data Breaches	Targeted Attack
		Simple Human Errors
		Application Vulnerabilities
		Poor Security Policies
T02	Data Loss	Natural Disasters
		Simple Human Errors
		Hard Drive Failures
		Power Failures
		Malware Infection
T03	Malicious Insiders	Former Employee
		System Administrator
		Third Party Contractor
		Business Partner
T04	Denial of Service (DoS)	Weak Network Architecture
		Insecure Network Protocol
		Vulnerable Application
T05	Vulnerable Systems and APIs	Weak API Credentials
		Key Management
		Operating System Bugs
		Hypervisor Bugs
		Unpatched Software
T06	Weak Authentication and Identity Management	Social Engineering Attacks
		Man-In-The-Middle (MITM) Attack
		Malware Infection
T07	Account Hijacking	Social Engineering Attacks
		Man-In-The-Middle (MITM) Attack
		Malware Infection
T08	Shared Technology Vulnerabilities	VM Vulnerabilities
		Hypervisor Vulnerabilities
		Third-Party S/W Vulnerabilities
T09	Lacking Due Diligence	No Auditing
		Service Level Agreement
T10	Advanced Persistent Threats (APT)	Spear Phishing or Whailing
		Direct Hacking
		USB Malware
		Network Penetration
		Third-Party APIs
T11	Abuse of Cloud Services	No Cloud Service Monitoring
		Service Level Agreement
T12	A Lack of Responsibility	Human Negligence
		Service Level Agreement
T13	Insufficient Security Tools	--
T14	Human Error	Human Negligence
		No or Insufficient Security Training
T15	Ransomware	Infrastructure Vulnerabilities
		Platform Vulnerabilities
		Application Vulnerabilities
T16	Spectre and Meltdown	Hardware Design

		Vulnerabilties
T17	Unprotected IoT Devices	Weak Device Management
		Network Vulnerabilities
		Hardware Vulnerabilities

Importance and impact of latest threats like Ransomware, Spectre and Meltdown are also presented. The future direction is to classify these threats along the cloud service delivery models and simulate the impact of some of these threats using various cloud simulators [2].

REFERENCES

[1] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, *"An analysis of security issues for cloud computing,"* J. Internet Serv. Appl., vol. 4, no. 1, p. 5, 2013.

[2] P. S. Suryateja, *"A Comparative Analysis of Cloud Simulators,"* Int. J. Mod. Educ. Comput. Sci., vol. 8, no. 4, pp. 64–71, 2016.

[3] *Tripwire Top Cloud Security Threats* - https://www.tripwire.com/state-of-security/security-data-protection/cloud/top-cloud-security-threats/ (last accessed on Mar, 2018)

[4] *CSOonline Top Cloud Security Threats 2018* - https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html (last accessed on Mar, 2018)

[5] *Comparethecloud 8 Public Cloud Security Threats* - https://www.comparethecloud.net/articles/8-public-cloud-security-threats-to-enterprises-in-2017/ (last accessed on Mar, 2018)

[6] *Tierpoint Top 5 Cloud Data Security Threats* - https://www.tierpoint.com/top-5-cloud-data-security-threats-in-2018/ (last accessed on Mar, 2018)

[7] *Techtarget Five Cloud Security Threats to Combat in 2018* - http://searchcloudcomputing.techtarget.com/tip/Five-cloud-security-threats-to-combat-in-2018 (last accessed on Mar, 2018)

[8] S. Bulusu, *"A Study on Cloud Computing Security Challenges,"* 2012.

[9] B. T. Rao, *"A Study on Data Storage Security Issues in Cloud Computing,"* Procedia - Procedia Comput. Sci., vol. 92, pp. 128–135, 2016.

[10] N. Khan and A. Al-yasiri, *"Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework,"* Procedia - Procedia Comput. Sci., vol. 94, pp. 485–490, 2016.

[11] G. Somani, M. Singh, D. Sanghi, M. Conti, and R. Buyya, *"DDoS attacks in cloud computing : Issues , taxonomy , and future directions,"* Comput. Commun., vol. 107, pp. 30–48, 2017.

[12] B. Varghese and R. Buyya, *"Next Generation Cloud Computing: New Trends and Research Directions,"* vol. 2017, no. September, pp. 1–22, 2017.

[13] B.SriVarsha, P.S.Suryateja, *"Using Advanced Encryption Standard for Secure and Scalable Sharing of personal Health Records in Cloud,"* International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5(6), 7745-7747, 2014.

Authors Profile

P. S. Suryateja is at present working as an Asst. Professor in CSE Dept. at Vishnu Institute of Technology, Bhimavaram, AP, India. His current research interests include cloud computing and network security. He is a member of ACM and lifetime member of CSI. He has 7 years of teaching experience and loves teaching, and learning new technologies.

