A Comprehensive Analysis of Risks, Threats and Vulnerabilities in Cloud Computing

Pranay Kumar BV

Associate professor Department of IT
Christu Jyothi Institute of Technology and science, Jangaon Warangal, India

Abstract: Cloud computing is new paradigm that's driving the world of technology and services over the Internet. Cloud providers facilitate individuals and businesses to use software and hardware that are managed by third parties at remote locations. Cloud services include online file storage, social networking sites, webmail, and online business Applications. Moving critical applications and sensitive data to public cloud environments is of great concern for those corporations that are moving beyond their data center's network under their control. To alleviate these concerns, a cloud solution provider must ensure that customers will continue to have the same security and privacy controls over their applications and services, provide evidence to customers that their organization are secure and they can meet their service-level agreements, and that they can prove compliance to auditors

Keywords: Cloud computing, Security, SPI model, Vulnerabilities, Threats, Countermeasures, regionalization, transparency.

I. Introduction

Recent Snowden leaks aren't driving companies away from the cloud and its services; but the disclosures have made them a lot more careful and present cloud providers have more to guarantee the security of the customer data and business. In today's world Cloud computing is the most sought after and popular technology. Cloud Computing enables 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. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters. Because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing.

Security concerns relate to risk areas such as external data storage, dependency on the public internet, lack of control, multi-tenancy and integration with internal security Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form. Security controls in Cloud Computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, Cloud Computing may present different risks to an organization than traditional IT solutions. Unfortunately, integrating security into these solutions is often perceived as making them more rigid.

A threat is defined as a potential attack that may lead to a misuse of information or resources, and vulnerability is the flaws allow an attack to be successful. This paper describes the relationship between these vulnerabilities and threats; how these vulnerabilities can be exploited in order to perform an attack, and also present some countermeasures related to these threats which try to solve or improve the identified problems.

II Literature Survey

2.1 Security in the SPI model [3] provides three types of services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

With SaaS, the burden of security lies with the cloud provider. In part, this is because of the degree of abstraction, the SaaS model is based on a high degree of integrated functionality with minimal customer control or extensibility. By contrast, the PaaS model offers greater extensibility and greater customer control. Largely because of the relatively lower degree of abstraction, IaaS offers greater tenant or customer control over security than do PaaS or SaaS [1].

Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. These relationships and dependencies between cloud models may also be a source of security risks. A SaaS provider may rent a development environment from a PaaS provider, which might also rent an infrastructure from an IaaS provider. Each provider is responsible for securing his own services, which may result in an inconsistent combination of security models. It also creates confusion over which service provider is responsible once an attack happens.

2.2 Software-as-a-Service (SaaS) Security Issues

SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM. SaaS users have less control over security among the three fundamental delivery models in the cloud. The adoption of SaaS applications may raise some security concerns.

2.3 Application Security

Applications are delivered via the Internet and a Web browser. However, flaws in web applications may create vulnerabilities for the SaaS applications. Attackers use the web to compromise user's computers and steal sensitive data. Security challenges in SaaS applications are same as web applications The Open Web Application Security Project (OWASP) has identified the ten most critical web applications security threats.

2.4 Multi-Tenancy

The applications in Saas are grouped into maturity models that are determined by the following characteristics: scalability, configurability via metadata, and multi-tenancy. In the first maturity model, each customer has his own customized instance of the software. In the second model, the vendor also provides different instances of the applications for each customer, but all instances use the same application code. In the third maturity model multi-tenancy is added, so a single instance serves all customers. This approach enables more efficient use of the resources but scalability is limited. Since data from multiple tenants is likely to be stored in the same database, the risk of data leakage between these tenants is high. Good Security policies are the need of the hour to guarantee that customer's data are kept separate from other customers.

2.5 Data Security

Data security in SaaS is managed by Cloud providers. Organizational data is processed in plaintext and stored where the provider is responsible for data security, Data backup and sub contract. Most compliance standards cannot be envisioned in a world of Cloud Computing [5]. In the world of SaaS, the process of compliance is complex because data is located in the provider's datacenters, which may introduce regulatory compliance issues such as data privacy, segregation, and security, that must be enforced by the provider.

2.6 Accessibility

Accessing applications over the internet via web browser makes access from any network device easier, including public computers and mobile devices. However, it also exposes the service to additional security risks. The Cloud Security Alliance [6] has released a document that describes the current state of mobile computing and the top threats in this area such as information stealing mobile malware, insecure networks (WiFi), vulnerabilities found in the device OS and official applications, insecure marketplaces, and proximity-based hacking.

2.7 Platform-as-a-Service (PaaS) Security Issues

PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers [3]. As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform [1]. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications. Same as SaaS, PaaS also brings data security issues and other challenges that are described as follows:

2.8 Infrastructure-as-a-Service (IaaS) Security Issues

IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet. Users are entitled to run any software with full control and management on the resources allocated to them. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor. They control the software running in their virtual machines, and they are responsible to configure security policies correctly. However, the underlying compute, network, and storage infrastructure is controlled by cloud providers. IaaS providers must undertake a substantial effort to secure their systems in order to minimize these threats that result from creation, communication, monitoring, modification, and mobility [07].

2.9 Shared Resource

VMs located on the same server can share CPU, memory, I/O, and others. Sharing resources between VMs may decrease the security of each VM. For example, a malicious VM can infer some information about other VMs through shared memory or other shared resources without need of compromising the hypervisor. Using covert channels, two VMs can communicate bypassing all the rules defined by the security module of the VMM. Thus, a malicious Virtual Machine can monitor shared resources without being noticed by its VMM, so the attacker can infer some information about other virtual machines.

2.13 Virtual Machine Rollback

Virtual machines roll back to the previous states if an error happens. But rolling back in virtual machines may lead to security vulnerabilities that were patched or re-enable previously disabled accounts or passwords. One solution is to make a “copy” (snapshot) of the virtual machine, but this will propagate configuration errors and other vulnerabilities.

2.16 Analysis of Security Issues in Cloud Computing

This section discusses security vulnerabilities and threats of Cloud Computing. For each vulnerability and threat, we identify what cloud service model or models are affected by these security problems. The focus is mainly technology-based vulnerabilities but some of the vulnerabilities that may be common to any organization and can show negative impact are:

1)Lack of employee screening and poor hiring practices 2)Lack of customer background checks –Apocryphal accounts can let attackers perform any malicious activity without being identified 3)Lack of security education

III Vulnerabilities

Cloud Computing leverages many existing technologies such as web services, web browsers, and virtualization, which contributes to the evolution of cloud environments. Therefore, any vulnerability associated to these technologies also affects the cloud, and it can even have a significant impact. Table 2 presents an analysis of vulnerabilities in Cloud Computing. This analysis offers a brief description of the vulnerabilities, and indicates what cloud service models (SPI) can be affected by them. For this analysis, we focus mainly on technology-based vulnerabilities; however, there are other vulnerabilities that are common to any organization, but they have to be taken in consideration since they can negatively impact the security of the cloud and its underlying platform. Some of these vulnerabilities are the following: Lack of employee screening and poor hiring practices, Lack of customer background checks, Lack of security education.

Cloud Computing leverages many existing technologies such as web services, web browsers, and virtualization, which contributes to the evolution of cloud environments. Therefore, any vulnerability associated to these technologies also affects the cloud, and it can even have a significant impact.

Table 1: Vulnerabilities in cloud computing

S.No	Vulnerability	Description	layer
V1	Insecure interfaces and APIs	Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML).The security of the cloud depends upon the security of these interfaces . Some problems are: a) Weak credential b) Insufficient authorization checks c) Insufficient input-data validation	SPI
V2	Unlimited allocation of resources	Inaccurate modeling of resource usage can lead to overbooking or over-provisioning.	SPI
V3	Data-related vulnerabilities	a) Data can be collocated with the data of unknown owners (intruders) with a weak separation b) Data may be located in different jurisdictions which have different laws c) Incomplete data deletion – data cannot be completely removed d) Data backup done by untrusted third-party providers e) Information about the location of the data usually is unavailable or not disclosed to users. f) Data is often stored, processed, and transferred in clear plain text	SPI

V4	Vulnerabilities in Virtual Machines	a) Possible covert channels in the collocation of VMs b) Unrestricted allocation and deallocation of resources with VMs [7]c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance [7] d) Uncontrolled snapshots – VMs can be copied in order to provide flexibility [5], which may lead to data leakage) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration [44], but patches applied after the previous state disappear f) VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography)	I
V5	Vulnerabilities in V.M Images	a) Uncontrolled placement of VM images in public repositories b) VM images are not able to be patched since they are dormant artifacts	I
V6	Vulnerabilities in Hypervisors	a) Complex hypervisor code b) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited	I
V7	Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines	I

We infer from the above table 2 that data storage and virtualization are the very critical and an attack to them can be more harmful. Attacks on lower layers have high impact than above layers.

IV Threats in Cloud Computing

Table 2: The following table describes various threats and their description

S.No	Threats	Description	layer
T1	Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction.	SPI
T2	Data scavenging	Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data.	SPI
T3	Data leakage	Data leakage happens when the data gets into the wrong hands when transferred, stored, audited or processed.	SPI
T4	Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.	SPI
T5	Customer-data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application [20,32]. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.	SPI
T6	VM escape	It is designed to exploit the hypervisor in order to take control of the underlying infrastructure.	I

T7	VM hopping	It happens when a VM is able to gain access to another VM (i.e. by exploiting some hypervisor vulnerability)	I
T8	Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository [20].	I
T9	Insecure VM migration	Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions: a) Access data illegally during migration [42] b) Transfer a VM to an untrusted host [44] c) Create and migrate several VM causing disruptions or DoS	I
T10	Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/ to other.	I

V Countermeasures

5.1 Countermeasures for T01: Account or Service Hijacking

Identity and access management guidance: Cloud Security Alliance (CSA), a non-profit organization that promotes the use of best practices in order to provide security in cloud environments and identity and access reporting.

Dynamic credentials: The dynamic credential changes its value once a user changes its location or when he has exchanged a certain number of data packets.

5.2 Countermeasures for T03: Data Leakage

A. Fragmentation-redundancy-scattering (FRS) technique: This technique aims to provide intrusion tolerance and, in consequence, secure storage. This technique consists in first breaking down sensitive data into insignificant fragments, so any fragment does not have any significant information by itself. Then, fragments are scattered in a redundant fashion across different sites of the distributed system.

B. Digital signatures: [8] proposes to secure data using digital signature with RSA algorithm while data is being transferred over the Internet. They claimed that RSA is the most recognizable algorithm, and it can be used to protect data in cloud environments.

C. Homomorphic encryption: Three important operations for cloud data are transfer, store, and process. Normally encryption may be used for to and fro transfer of data .The method is based on the application of fully homomorphic encryption to the security of clouds. Fully homomorphic encryption allows performing arbitrary computation on cipher texts without being decrypted. Current homomorphic encryption schemes support limited number of homomorphic operations such as addition and multiplication but real-world cloud applications requires a huge processing power which may impact on user response time and power consumption.

D. Encryption: Encryption techniques have been used for long time to secure sensitive data. Sending or storing encrypted data in the cloud will ensure that data is secure. However, it is true assuming that the encryption algorithms are strong. There are some well-known encryption schemes such as AES (Advanced Encryption Standard). Also, SSL technology can be used to protect data while it is in transit. Moreover, [9] describes that encryption can be used to stop side channel attacks on cloud storage de-duplication, but it may lead to offline dictionary attacks reveling personal keys.

5.3 Countermeasures for T05: customer data manipulation : Web application scanners: Web application scanners is a program which scans web applications through the web front-end in order to identify security vulnerabilities such as web application firewall which routes all web traffic through the web application firewall which inspects specific threats.

5.4 Countermeasures for T06: VM Escape

A. Hyper Safe : Hyper Safe's goal is to protect type I hypervisors using two techniques: non-by by passable memory lockdown which protects write-protected memory pages from being modified, and restricted pointed indexing that converts control data into pointer indexes.

B. Trusted cloud computing platform:TCCP enables providers to offer closed box execution environments, and allows users to determine if the environment is secure before launching their VMs. The TCCP adds two fundamental elements: a trusted virtual machine monitors (TVMM), and a trusted coordinator (TC). The TC manages a set of trusted nodes that run TVMMs, and it is maintained but a trusted third party. The TC participates in the process of launching or migrating a VM, which verifies that a VM is running in a trusted platform.

5.5 Countermeasures for T08: malicious virtual machine creation: Mirage: A virtual machine image management system approach includes the following security features: access control framework, image filters, a provenance tracking, and repository maintenance services. However, the limitation of this approach is that filters may not be able to scan all malware or remove all the sensitive data from the images. Also, running these filters may raise privacy concerns because they have access to the content of the images which can contain customer's confidential data.

VI Conclusions

Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users.

New security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies.

Despite some reports of slowing sales of cloud services by U.S. vendors to overseas companies, experts now expect that the Snowden leaks will have little effect on long-term sales. Analysis say IT security officials are looking at several key areas, such as data encryption, key management and data ownership, regionalization, and the need for increased government transparency, to improve cloud security. Encryption is only as secure as its key management system. US data leaks could also accelerate regionalization of cloud services. Data residency requirements is becoming the order of the day

VII Acknowledgments

I would like to express my gratitude and heartfelt thanks to Rev.Fr.Y Papi Reddy for his constant mentoring, Dr.JBV Subramnayam for his guidance and my colleagues for their support in authoring this paper.

VIII References

1. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly
2. Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0.Available: https://cloudsecurityalliance.org/research/top-threats
3. Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1)
4. Zhang Y, Liu S, Meng X (2009) towards high level SaaS maturity model
5. Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security
6. Cloud Security Alliance (2012) Security guidance for critical areas of Mobile Computing.
7. Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: Challenges and solutions. In: the 7th International Conference onInformatics and Systems (INFOS), Potsdam, Germany. IEEE Computer Society, Washington, DC, USA, pp 1–8
8. Somani U, Lakhani K, Mundra M (2010) Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing. In: 1st International conference on parallel distributed and grid Computing (PDGC). IEEE Computer Society Washington, DC, USA, pp 211
9. Harnik D, Pinkas B, Shulman-Peleg A (2010) Side channels in Cloud services: deduplication in Cloud Storage. IEEE Security Privacy 8(6)