A Study on Cloud Computing Challenges and Analysis of Security Issues

Dr. S.K. Singh
Amity University, Lucknow Campus, Lucknow, INDIA

Abstract
Cloud Computing is a flexible, cost-effective, and reliable delivery platform for providing IT services to business or consumer over Internet. It is a collection of distributed services, application, information and infrastructure. It is defined as the set of services that provide infrastructure resources using internet and data storage on a third server. It provides its user scalability, reliability, high performance and low cost solution compared to the other infrastructure. However, cloud Computing have an added level of risk because essential services are often outsourced to a third party, hence harder to maintain data security and privacy, support data and service availability. We discuss here, vulnerabilities and relate threats with possible solutions on reviewing algorithms.

Keywords--- Cloud computing, security, privacy, virtualization, Threats, vulnerability.

I. INTRODUCTION

A study by Gartner considered Cloud Computing as the first among the top 10 most important technologies and with a better prospect in coming years by almost all companies and organizations.

Cloud computing is now known for accessing resources from a pool which is owned and maintained by a third party vendor using internet. It is a technology which keeps up data using internet and remote servers. In cloud computing generally resources are kept in someone else’s authority and are accessed remotely by the user. It is a type of computing that depends on sharing of data. The term cloud computing is originated as a metaphor for the Internet which is, in essence, a network of networks providing remote access to a set of decentralized IT resources.

Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service with all computing resources visualized as services and delivered over the Internet.

The cloud enhances agility, availability, collaboration, scalability, ability to adapt to fluctuations according to demand, accelerate development work, and provides scope for cost reduction through optimized and efficient computing.

While there are many benefits to adopting Cloud Computing and also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters.

Security concerns relate to risk areas such as external data storage, lack of control, multi-tenancy, dependency on the “public” internet and integration with internal security.

Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form.

Moving critical applications and sensitive data to public cloud environments is of great concern for those organisations 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.

II. SECURITY ISSUES IN CLOUD

Security is the major concern in the cloud computing. The primary security issues faced in cloud computing are categorized as follows:

i) Privacy: It is the most important issue while discussing cloud computing. If a client host his data on the cloud there is always a concern of data privacy.
ii) Data integrity: the data integrity method must be included in cloud computing so that users have the awareness of where the data is hosted.

iii) Data location and relocation: cloud computing requires a high degree of data mobility. Generally in cloud computing consumer does not know about the location of data. If they wish to reside on the preferred location of data then in that case an agreement is signed between the cloud provider and the consumer to reside on a given server.

iv) Availability: data in the cloud is stored in the different locations unknown to the user, therefore availability of the uninterrupted data becomes a major issue in cloud computing.

v) Storage: when a user wants to move data to the cloud, he must be ensured about the adequate storage system.

The cloud model provides three types of services

**Software as a Service (SaaS).**

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

**Platform as a Service (PaaS).**

The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.

**Infrastructure as a Service (IaaS).**

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

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.

Analyzing security challenges in Cloud Computing, needs to understand the relationships and dependencies between these cloud service. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of these deep dependencies, any attack to any cloud service layer can compromise the upper layers. 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.

Basically security issues are within the domain of Software-as-a-service (SaaS) security issues, Application security, Multi-tenancy, Data security, Accessibility, Platform-as-a-service (PaaS) security issues, Infrastructure-as-a-service (IaaS) security issues.

**Analysis of security issues in cloud computing**

Existing security vulnerabilities and threats of Cloud Computing are tabulates below. For each vulnerability and threat, cloud service model or models are identified.

Table 1 presents an analysis of technology based vulnerabilities in Cloud Computing; 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 – some cloud providers may not perform background screening of their employees or providers. Privileged users such as cloud administrators usually have unlimited access to the cloud data.
- Lack of customer background checks – most cloud providers do not check their customer’s background, and almost anyone can open an account with a valid credit card and email. Apocryphal accounts can let attackers perform any malicious activity without being identified.
- Lack of security education – people continue to be a weak point in information security. This is true in any type of organization; however, in the cloud, it has a bigger impact because there are more people that interact with the cloud: cloud providers, third-party providers, suppliers, organizational customers, and end-users.

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.

**Vulnerabilities in cloud computing:**

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insecure interfaces and APIs</td>
<td>Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON). The security of the cloud depends upon the security of these interfaces. Some problems are:</td>
</tr>
<tr>
<td></td>
<td>a) Weak credential</td>
</tr>
<tr>
<td></td>
<td>b) Insufficient authorization checks</td>
</tr>
</tbody>
</table>
### Vulnerabilities

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c) Insufficient input-data validation</td>
</tr>
</tbody>
</table>

Also, cloud APIs are still immature which means that are frequently updated. A fixed bug can introduce another security hole in the application.

### Unlimited allocation of resources

Inaccurate modeling of resource usage can lead to overbooking or over-provisioning.

### Data-related vulnerabilities

- a) Data can be collocated with the data of unknown owners (competitors, or 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

### Vulnerabilities in Virtual Machines

- a) Possible covert channels in the colocation of VMs
- b) Unrestricted allocation and deallocation of resources with VMs
- c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance
- d) Uncontrolled snapshots – VMs can be copied in order to provide flexibility, which may lead to data leakage
- e) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration, 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)

### Vulnerabilities in Virtual Machine Images

- a) Uncontrolled placement of VM images in public repositories
- b) VM images are not able to be patched since they are dormant artifacts

### Vulnerabilities in Hypervisors

- a) Complex hypervisor code
- b) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited

### Sharing of virtual bridges by several

We can conclude that data storage and virtualization are the most critical and an attack to them can do the most harm. Attacks to lower layers have more impact to the other layers.

Table 2 presents an overview of threats in Cloud Computing. Like Table 1 it also describes the threats that are related to the technology used in cloud environments. We put more emphasis on threats that are associated with data being stored and processed remotely, sharing resources and the usage of virtualization.

### Threats in cloud computing

<table>
<thead>
<tr>
<th>Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account or service hijacking</td>
<td>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.</td>
</tr>
<tr>
<td>Data scavenging</td>
<td>Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data.</td>
</tr>
<tr>
<td>Data leakage</td>
<td>Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>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.</td>
</tr>
<tr>
<td>Customer-data manipulation</td>
<td>Users attack web applications by manipulating data sent from their application component to the server’s application. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.</td>
</tr>
<tr>
<td>VM escape</td>
<td>It is designed to exploit the hypervisor in order to take control of the underlying infrastructure.</td>
</tr>
<tr>
<td>VM hopping</td>
<td>It happens when a VM is able to gain access to another VM (i.e. by exploiting some hypervisor vulnerability)</td>
</tr>
<tr>
<td>Malicious creation</td>
<td>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.</td>
</tr>
</tbody>
</table>
has identified "The Notorious Nine," the top nine cloud-related threats lie. The algorithms used in cloud management processes that support use of the algorithms in cryptographic systems together with the key management processes that support use of the algorithms in some application context. The algorithms used in cloud computing as follows:

**i) Symmetric Encryption Algorithms:**

In this type of encryption, the sender and the receiver agree on a secret (shared) key. Then they use this secret key to encrypt and decrypt their sent messages. The related symmetric algorithms are:
- DES: The Data Encryption Standard, BLOWFISH, RC5, 3DES, AES

**ii) Asymmetric Algorithms:**

Asymmetric algorithms (public key algorithms) use different keys for encryption and decryption, and the decryption key cannot be derived from the encryption key. Asymmetric algorithms are important because they can be used for transmitting encryption keys or other data securely even when the parties have no opportunity to agree on a secret key in private. The related asymmetric algorithms are:
- RSA: Rivest-Shamir-Adleman
- DSA: Digital Signature Algorithm
- DIFFIE-HELLMAN
- EIGamal Algorithm

### III. EXISTING ALGORITHMS FOR SECURITY

Encryption plays a major role in secure data communication. Encryption is the process of converting plain text "unhidden" to a cryptic text "hidden" to secure it against data thieves. Cryptographic system is "a set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context." The algorithms used in cloud computing as follows:

**Insecure migration VM**

- 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
  b) Transfer a VM to an untrusted host
  c) Create and migrate several VM causing disruptions or DoS

**Sniffing/Spoofing virtual networks**

A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs.

### IV. CLOUD COMPUTING CHALLENGES

Cloud computing has grabbed the spotlight if we refer to RSA Conference 2013 in San Francisco, with vendors aplenty hawking products and services that equip IT with controls to bring order to cloud chaos. But the first step is for organization to identify precisely where the greatest cloud-related threats lie.

To that end, the CSA (Cloud Security Alliance) has identified "The Notorious Nine," the top nine cloud computing threats. 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.

First on the list is data breaches. To illustrate the potential magnitude of this threat, CSA pointed to a research paper from last November describing how a virtual machine could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server. A malicious hacker wouldn't necessarily need to go to such lengths to pull off that sort of feat, though. If a multitenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but every other clients' data as well.

The challenge in addressing these threats of data loss and data leakage is that "the measures you put in place to mitigate one can exacerbate the other," according to the report. You could encrypt your data to reduce the impact of a breach, but if you lose your encryption key, you'll 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.

The second-greatest threat in a cloud computing environment, according to CSA, is data loss: the prospect of seeing your valuable data disappears into the ether 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.

Data loss isn't only problematic in terms of impacting relationships with customers, the report notes. You could also get into hot water with the feds if you're legally required to store particular data to remain in compliance with certain laws, such as HIPAA.

The third-greatest cloud computing security risk is account or service traffic 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," according to the report. As an example, XSS attack on Amazon in 2010 that let attackers hijack credentials to the site.

The key to defending against this threat is to protect credentials from being stolen. "Organizations should look to prohibit the sharing of account credentials between users and services, and they should leverage strong two-factor authentication techniques where possible.".

Fourth on the list of threats are insecure interfaces and APIs. It administr 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

Denial of service ranks as the fifth-greatest security threat to cloud computing. DoS has been an Internet threat for years, but it becomes more problematic in the age of cloud computing when organizations are dependent on the 24/7 availability of one or more services. 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'll be forced to take it down yourself," the report says.

Sixth on the list is malicious insiders, which can be a current or former employee, a contractor, or a business partner who gains access to a network, system, or data for malicious purposes. 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." Seventh on the list is cloud abuse, such as a bad guy using a cloud service to break an encryption key too difficult to crack on a standard computer. Another example might be a malicious hacker using cloud servers to launch a DDoS attack, propagate malware, or share pirated software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes for identify it.

Eight on the list of top security threats to cloud computing is insufficient due diligence; that is, organizations embrace the cloud without fully understanding the cloud environment and associated risks. For example, entering the cloud can generate contractual issues with providers over liability and transparency. What's more, operational and architectural issues can arise if a company's development team isn't sufficiently familiar with cloud technologies as it pushes an app to the cloud. Virtual networks are also target for some attacks especially when communicating with remote virtual machines.

If an integral component gets compromised -- say, a hypervisor, a shared platform component, or an application -- it exposes the entire environment to a potential of compromise and breach. It is recommended that a defensive, in-depth strategy, including compute, storage, network, application, and user security enforcement, as well as monitoring.

V. CONCLUSION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since 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 vulnerability and threats security issues for cloud models: IaaS, PaaS, and SaaS, which vary depending on the model. As per analysis 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. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines.

Some surveys have discussed security issues about clouds without making any difference between vulnerabilities and threats. We have focused on this distinction, where we consider important to understand these issues. So we can identify what vulnerabilities contribute to the execution of these threats and make the system more robust. Also, some existing and current algorithm are listed in order to mitigate these threats. However, 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. In future we will produce the possible security technique which will best fit for changing cloud architectures.

REFERENCES


