Cloud Security: Challenges, Vulnerabilities and Solutions

Akshay Gujjar
California State University, Long Beach
Long Beach, California
Email: Akshay.Gujjar@student.csulb.edu

***Abstract*—There are several potential gains that can be achieved using cloud computing. Despite this, the security aspect of the cloud is still questionable. As new dimensions have entered the module, the security problem gets more complicated. Through the internet, the cloud service provider provides many services and resources. The transformation of local computing to cloud computing has brought many new challenges and hurdles for both the customer and the provider. A detailed analysis of the cloud security issues is done in this paper. The paper also explores the various concepts related to cloud security that are essential to understand the various security issues. The solutions to the threats, issues and problems are also covered.**

***Index Terms*—cloud, cloud computing, cloud security, cloud security challenges, cloud security issues, cloud security threats, cloud security solutions,**

I. Introduction

Cloud Computing is rapidly transforming the IT landscape. Cloud consumers can access various resources, applications, infrastructure provided by cloud providers on a pay-as-you-use basis. On top of that, massive storage infrastructure is available for the storage of data. Cloud Computing provides increased flexibility. For example, if you need extra storage or extra bandwidth, you can get that instantly, without the need for extra hardware by the user. Also mobility, like being able to access the internet on our phones is possible. There will always be things that are completely out of your control. In events like power outages or natural disasters cloud computing provides quick recovery of data. When data is stored locally and not on the cloud, there is always a chance of loss of data. Using cloud computing, data loss can be prevented. Another advantage is automatic software updates. Cloud computing can also be used to develop and deploy user applications. Cloud computing is used to provide a large number of on-demand services over the internet. This is achieved with the help of a large amount of virtual storage. Another advantage is that there is no setup cost of expensive computing infrastructure. Cloud computing has given a new meaning to distributed computing and completely changed distributed computing. It has also increased flexibility and scalability for computer processes. It is easy to back-up and restore data using Cloud Computing.

II. Service Models

In Cloud Computing, Service Models facilitate a list of services that are issued by the provider and consumed by the consumer. There are three service models. They are:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

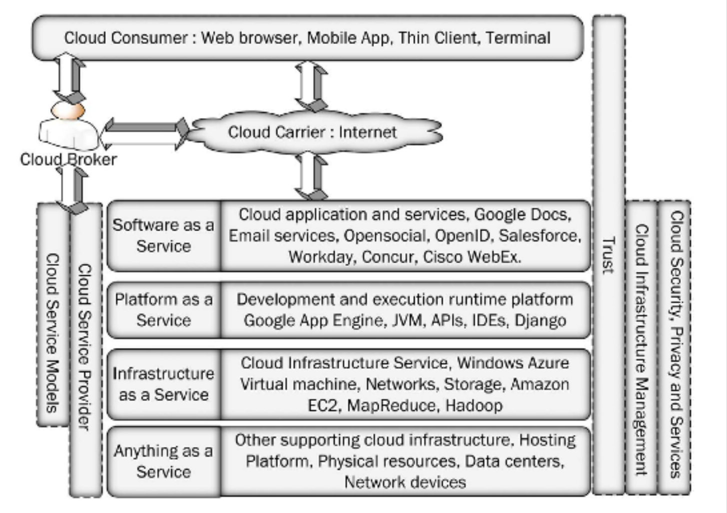
Cloud Consumer : Web browser, Mobile App, Thin Client, Terminal
Cloud Carrier : Internet
Cloud Broker
Cloud Service Models
Cloud Service Provider
Software as a Service
Cloud application and services, Google Docs, Email services, Opensocial, OpenID, Salesforce, Workday, Concur, Cisco WebEx.
Platform as a Service
Development and execution runtime platform Google App Engine, JVM, APIs, IDEs, Django
Infrastructure as a Service
Cloud Infrastructure Service, Windows Azure Virtual machine, Networks, Storage, Amazon EC2, MapReduce, Hadoop
Anything as a Service
Other supporting cloud infrastructure, Hosting Platform, Physical resources, Data centers, Network devices
Trust
Cloud Infrastructure Management
Cloud Security, Privacy and Services

Fig. 1. A Complete Cloud Computing Architectural Framework [1] Singh, Ashish, and Kakali Chatterjee. ”Cloud security issues and challenges: A survey.” Journal of Network and Computer Applications 79 (2017): 88-115.

A. Software as a Service (SaaS)

In SaaS, an Integrated Development Environment (IDE) is issued to a client for accessing applications and transferring data to a remote storage server with the aid of online software services. Examples of Software as a Service (SaaS) include Customer Relationship Management (CRM) and Salesforce.com.

B. Platform as a Service (PaaS)

In Platform as a Service (PaaS), a higher level of programmable platform is provided. Multiple programming models, an Integrated Development Environment (IDE), platform level resources, operating systems and specialized services are provided. The clients can create, execute, deploy, and manage their applications. One of the best examples of Platform as a Service (PaaS) is Google App Engine. Using Google App Engine, developers can develop and host web applications.

C. Infrastructure as a Service (IaaS)

In Infrastructure as a Service (IaaS), virtualized resources are offered by the cloud service provider for on-demand computations, network, storage, memory, communication, and processor. Example of Infrastructure as a Service (IaaS) is Amazon Web Services (AWS). AWS provides EC2 services like virtual machine (VM) to the customer.

III. Deployment Models

In Cloud Computing, Deployment Models describe the types of cloud. There are three deployment models. They are:

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud

A. Private Cloud

In Private Cloud, operations and maintenance are done internally by a single organization or by a Third Party Auditing (TPA).

B. Public Cloud

In Public Cloud, operations and management is done by the cloud service provider. The physical infrastructure of Public Cloud is at the off-site location of the user. Multiple users share the cloud resources and pay the cloud service provider according to their usage.

C. Community Cloud

In Community Cloud, a cloud is deployed and shared by a group of users that share a common interest such as security application, services, mission.

D. Hybrid Cloud

In Hybrid Cloud, two or multiple clouds with the same infrastructure and capabilities are mixed.

IV. Storage Models

Storage Models tell us how data is stored in the cloud. They also tell us about the availability of storage space. In the cloud environment, there are many types of storage solutions. Each solution has its own pros and cons. A consumer can choose a solution based on their requirement and available data. There are three main types of Storage Models. They are:

- Shared File/Block Storage System
- Object Storage System
- Database or Table Storage System

A. Shared File/Block Storage System

In Shared File/Block Storage System, multiple users/hosts share data located in files and folders, using the Internet. Standard protocols and capabilities are used. The popular protocols used for storing and accessing data are Network File System (NFS), Server Message Block (SMB), and Common Internet File System (CIFS).

B. Shared File/Block Storage System

In Object Storage System, data is stored in the form of objects. Global key, Hash or Uniform Resource Locator (URL) is used to access every object using Representational State Transfer (REST) or web service-based cloud services. An object storage interface for accessing objects is provided by Cloud Data Management Interface (CDMI).

C. Object Storage System

In Object Storage System, data is stored in the form of objects. Global key, Hash or Uniform Resource Locator (URL) is used to access every object using Representational State Transfer (REST) or web service-based cloud services. An object storage interface for accessing objects is provided by Cloud Data Management Interface (CDMI).

D. Database or Table Storage System

Many cloud service providers store data in Relational Database Management Systems (RDBMs) in the form of rows and columns. In relational databases, data integrity is maintained and data redundancy is avoided. In cloud-based relational databases, scaling and performance is the major issues.

V. Cloud Security Concepts

In cloud security, various security issues and threats are covered. It is important to understand these security issues and threats to understand the concept of cloud security. In this paper, some of the cloud specific concepts are covered to understand the security issues present in the cloud. Some of the important cloud security concepts are:

- Virtualization Aspect
- Multi-tenancy
- Data Outsourcing

A. Virtualization Aspect

Virtualization is the process of extracting the services, computing resources, applications, operating system from the hardware on which they run. The two main components are virtualization are Virtual Machines (VMs) and Virtual Machine Managers (VMMs). A Virtual Machine (VM) is an image of an operating system called guest operation system. Multiple programs run on the guest OS. However, a guest OS does not provide direct access to the hardware. The Virtual Machine Managers (VMMs) are responsible for allocation of virtual hardware resources including CPUs, hard disk, network, and memory to each VM.

B. Multi-tenancy

The sharing concept is introduced in multi-tenancy, where each running instance can be shared by multiple users called tenants. Multi-tenancy provides the capability to share a single cloud platform by multiple users. In Infrastructure as a Service (IaaS), Virtual Machine Managers (VMMs) is referred to a multi-tenancy sharing platform whereas Virtual Machines (VMs) refers to the instances. In Platform as a Service (PaaS), a Virtual Platform (VP), enables a user to execute multiple applications such as Java Virtual Machine (JVM) and .NET parallelly in a multi-tenancy environment.

C. Data Outsourcing

Data Outsourcing refers to a mechanism where the responsibility of data extraction and collection over a certain subject to a third party. The third-party usually works on a contractual basis. Data Outsourcing provides both capital and operational investment. Many IT industries have adopted the Data Outsourcing concept. There are some drawbacks to Data Outsourcing. Firstly, a physical separation is created between the user and their data. Secondly, the client loses control over their data. When a customer gives their data to a third party, it must be ensured that storage and data computing are being done in a secure manner.

VI. Requirements of Cloud Security

Before choosing any of the cloud services, each business organization chooses some security strategy. The six main security requirements are: authentication or identification, authorization, confidentiality, integrity, non-repudiation, and availability. To prohibit unauthorized access, each service model, i.e., SaaS, PaaS, and IaaS requires authorization. Hybrid clouds offer more security compared to public and private clouds because hybrid clouds require higher security parameters compared to public and private clouds. In hybrid cloud, the integration options also add an extra layer of security. Integrity is a major requirement in all security models for checking the correctness of data.

VII. Threats to Cloud Computing

Anything that can cause serious harm to a computer system is defined as a threat. Potential attacks on the computer system or network infrastructure can be caused due to threats. Some of the treats to cloud computing are:

- Data Loss and Leakage
- Insecure Interface and API
- Identity Theft

A. Data Loss and Leakage

Data loss refers to the deletion, alteration, or theft of data without any backup of the original content. Data loss can also be produced by loss of an encoding key, due to the sharing and productive nature of cloud computing. Data Loss and Leakage can be caused by lack of authentication, access control, authorization, weak keys, weak encryption algorithms, unreliable data centers, risk of association and risk of association. Prevention methods for Data Loss and Leakage include having a secure API, secure storage, strong encryption key and algorithms, and data backup.

B. Insecure Interface and API

A set of software services and APIs are provided by the cloud service provider to their users for communication with the cloud services. The interfaces are in the form of a layer, located top of the cloud framework. This increases the complexity of the cloud. The security of the APIs is very important for the security and availability of the cloud. The security of these APIs can be reduced by both accidental and malicious attempts. The treats can also be magnified since other third parties can also build on top of these APIs. Secure interface models, adoption of proper authentication and access control mechanism can be adopted for preventing this.

C. Identity Theft

Identity theft refers to a type of trickery where someone impersonated the identity of a legitimate user. The impersonator steals the credits and associated resources of the victim. Due to this threat, the victim suffers many unwanted results and losses. Reasons for Identity Theft include weak password recovery method, key-loggers, phishing attacks, etc.

VIII. Attacks on Cloud Security

The value of cloud computing in a business environment is invaluable, and companies know that. New technologies are emerging, and new attacks are being formulated. Some of the common cloud security attacks include:

- Denial of Service Attack
- Distributed Denial of Service Attack (DDoS Attack)
- Service Injection Attack

A. Denial of Service Attack

In this type of attack, the attacker sends a large number of request packets to the victim, with the aid of the internet. The attacker's main aim is to exhaust all resources of the victim. The attacker floods a large number of requests to performance, computational power and cryptographic operations of the user.

B. Distributed Denial of Service Attack (DDoS Attack)

There is another type of attack known as Distributed Denial of Service Attack (DDoS Attack). A DDoS attack is much more complex and harder to detect compared to Denial-of-Service attack. In DDoS attack, the attacker, also known as controller, scans the entire network and makes a list of all the handlers, i.e., defenseless hosts. Each handler then creates or recruits multiple agents called zombies to launch attacks.

C. Service Injection Attack

The cloud system is responsible for offering services to its user. Every time a user needs access to a service, the user sends a request to the cloud. The cloud system then provides the resources for the requested service. The new allocated resource may later be assigned to another requesting user. In Service Injection Attack , the attacker makes a new malicious image of the assigned resource and tries to inject the malicious service or resource into the cloud environment. This can cause harm to the cloud environment and may cause the cloud to malfunction. A service integrity module must be implemented to prevent this type of attack.

IX. Cloud Security Issues and Solutions

A security issue can be defined as something that occurs due to misconfiguration, fault, damage, loopholes, and weakness in the system. Some of the security issues are:

- Data Storage
- Un-trusted Computing
- Cryptography
- Internet and Services related Security Issues

A. Data Storage

Data is a vital part of cloud computing. In the data storage issue, loss of control is a major issue in cloud computing model because it does not provide full control over the data, and it is harder to check data integrity and confidentiality. Organizations like Amazon and Google store their data based on multi-location feature that can bring new security threats and legal problems, as the data stored across the world have different policies. The solutions to these problems varies depending upon the nature of the problems.

B. Un-trusted Computing

When an application called another application or service, A service tree is generated. Simply put, the request is sent from one service to another service and so on. A computing framework that computes large data sets in distributed system may produce the unwanted, inaccurate, and dishonest result due to misconfiguration and malicious servers. It is hard to find an honest and accurate computation server that gives an accurate and honest results.

C. Cryptography

The bad implementation of the algorithm or usage of a weak key in the encryption can increase the possibility of attacks. Cryptosystems like RSA can be used for stronger encryption, which uses the prime factorization of a large number.

D. Internet and Services related Security Issues

The Internet is a carrier that transmits a large number of packets from source to destination in the form of digital data. The data are passed through several nodes, so it is not safe. The internet exploits many issues like IP spoofing, port scanning, malware injections, and packet sniffing. The web and standard web browsers are not the safest options for end users. Internet security challenges come with many solutions, but there are also newer evolving problems.

X. Conclusion

In this paper, the basic features of cloud computing as well as security issues were mentioned. There are many issues that originate due to the public, shared, distributed and virtualized nature of cloud computing. However, there are many advantages as well. The multi-tenancy and virtualization features allow the users to access the same resources from different locations. It is very much evident that cloud computing is a rapidly emerging technology and it is widely accepted all over the world. It is essential for all users to be aware of the vulnerabilities, threats and attacks that exist in the cloud.

References

[1] Singh, Ashish, and Kakali Chatterjee. ”Cloud security issues and challenges: A survey.” Journal of Network and Computer Applications 79 (2017): 88-115.

[2] I. Odun-Ayo, M. Ananya, F. Agono and R. Goddy-Worlu, ”Cloud Computing Architecture: A Critical Analysis,” 2018 18th International Conference on Computational Science and Applications (ICCSA), 2018, pp. 1-7, doi: 10.1109/ICCSA.2018.8439638.

[3] A. Behl, ”Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation,” 2011 World Congress on Information and Communication Technologies, 2011, pp. 217-222, doi: 10.1109/WICT.2011.6141247

[4] A. Bouayad, A. Blilat, N. E. H. Mejhed and M. El Ghazi, ”Cloud computing: Security challenges,” 2012 Colloquium in Information Science and Technology, 2012, pp. 26-31, doi: 10.1109/CIST.2012.6388058.