Cloud Computing: Security Issues and Security Standards

Shaireen Khan¹, Shadab Hasan², Shashank Singh³, Sumera Zafar⁴ and Shobhit Joshi⁵
¹,²,³,⁴,⁵ Computer Science and Engineering, Integral University, Lucknow, INDIA

ABSTRACT
A Cloud contains a huge pool of assets, which could be reallocated to various purposes inside brief time allotments, and enables the cloud proprietor to profit altogether from economies of scale and in addition from factual multiplexing. Cloud benefits today are conveyed in easy to use way and offered on a remarkable scale. Cloud computing is being touted a following best thing for cutting the cost of giving top notch IT services. Cloud computing utilizes item based equipment as its base. Cloud Platform is utilized both in modern field and scholastic field. The expansion in the cloud computing condition likewise expands security issues and difficulties for cloud engineers. Clients of cloud spare the data in the cloud, the absence of data protection in cloud can loose the client’s trust.
In this paper it is discussed some of the issues in cloud computing and techniques that are needed for the security of the data in the cloud. There are also Cloud Security Standards made to processes for implementing a security program.

Keywords:  Cloud Computing, Cloud Platform, Security Issues, Data Protection, Cloud Security, Cloud Security Standards

I. INTRODUCTION
Cloud Computing is an emerging style of computing where applications, data, and resources are provided to users as services over the Web. The services provided may be available globally, always on, low in cost, ‘on demand’, massively scalable, ‘pay-as-you-grow’.[4] Consumers of a service need to care only about what the service does for them, and not on how it is implemented. Cloud computing is a technology that allows users to access software applications, store information, develop and test new software, create virtual servers, draw on disparate IT resources, and more - all over the Internet (or other broad network).
utilization of a single organization. Private cloud services are dedicated for a single organization.[6] Cloud infrastructure can be setup on premise or off-premise and may be managed internally or by a third-party. Private clouds are best suited for applications where security is very important and organizations that want to have very tight control over their data.

Hybrid Cloud: Hybrid clouds combine elements of public and private clouds. The individual clouds retain their unique identities but are bound by institutionalized or restrictive innovation that empowers data and application probability. [6] Hybrid clouds are best suited for organizations that want to take advantage of secured application and data hosting on a private cloud, and at the same time benefit from cost savings by hosting shared applications and data in public clouds.

Community Cloud: In the community cloud development model, the cloud services are shared by several organizations that have the same policy and compliance considerations [6]. Community clouds are best suited for the organizations that want access to the same applications and data, and want the cloud costs to be shared with the larger group.

B. Service Models

Cloud services can be divided into three categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Infrastructure-as-a-Service (IaaS): IaaS gives the client the ability to arrange computing and storage resources. These resources are provided to the users as virtual machine instances and virtual storage. Users can start, stop, configure and manage the virtual machine instances and virtual storage. Users can deploy operating systems and applications of their choice on the virtual resources provisioned in the cloud. The cloud service provider manages the underlying infrastructures. Virtual resources provisioned by the users are billed based on a pay-per-use paradigm. Common metering metrics used are the number of virtual machine hours used and/or the amount of storage space provisioned.

Platform-as-a-Service (PaaS): PaaS provides the users the capability to develop and deploy application in the cloud using the development tools, application programming interfaces (APIs), software libraries and services provided by the cloud service provider. The cloud service organization deals with the fundamental cloud infrastructure including servers, network, operating systems and storage. The users, themselves are responsible for developing deploying configuring and managing applications on cloud infrastructure.

Software-as-a-Service (SaaS): Provide the user complete software application or the user interface to the application itself. The cloud specialist co-op deals with the basic cloud infrastructure including servers network, operating systems, storage and application software, and the user is unaware of the underlying architecture of the cloud. Applications are provided to the user through a thin client interface (e.g., a browser). SaaS applications platform independent and can be accessed from various client devices such as workstations, laptop, tablets and smartphones, running different operating systems. Since the cloud service provider manages the both the application and data, the users are able to access the applications from anywhere.

II. CLOUD SECURITY ISSUES

Organization uses various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and administrations has different security issues. Each administration demonstrate is related with a portion of the issues. Security issues are considered in two perspectives. To begin within the perspective of specialist co-op who protects that administrations gave by them ought to be secure and furthermore deals with the client's character administration. Other view is client see that guarantees that administration that they are utilizing is sufficiently secure.

A. Multi-Tenancy

As long as the cloud supplier assembles its security to meet the higher-chance customer, the greater part of the lower-hazard customers show signs of improvement security than they would have typically. A swathe producer may have a generally safe of being an immediate focus of malefactors, yet a music mark that is as of now utilizing document sharers could have a high danger of being focused by malefactors. At the point when both the wrap producer and the music mark utilize a similar cloud (multi-tenancy), it is conceivable that assaults coordinated at the music name could influence the gauze maker's foundation also. So the cloud supplier must...
outline the security to address the issues of the music name - and the gauze maker gets the advantages.

B. Elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the abilities accessible for provisioning regularly give off an impression of being boundless and can be acquired in any amount whenever.

C. Insider attacks

Cloud display is a multi-tenant based model that is under the supplier's single administration areas. This is a danger that emerges inside the association. There are no contracting norms and suppliers for cloud employees [1]. So an outsider merchant can without much of a stretch hack the information of one association and may degenerate or pitch that information to other association.

D. Outsider attacks

This is the one of the major concerning issue in an association since it discharges the private data of an association in open. Clouds are not like a private system, they have a larger number of interfaces than private system. So hackers and attackers have favorable position of misusing the API, shortcoming and may complete an association breaking [1].These assaults are less unsafe than the insider assaults in light of the fact that in the later we here and there unfit to recognize the attack.

E. Loss of control

Cloud utilizes a location transparency model by which it empower associations to unaware about the area of their services and data. Subsequently provider can have their administrations from anywhere in the cloud. For this situation association may lose their information and potentially they don't know about security instrument set up of the provider.

Figure V. Loss of control [1]

F. Data Leakage

Data Leakage has become one of the greatest organizational risks from a security standpoint. Virtually every legislature worldwide has controls that order assurances for specific data types [4].

The cloud provider should have the ability to outline approach to the security command clients must consent to and examine the issues. At a minimum, the data that falls under legislative mandates, or contractual obligation, should be encrypted while in flight and at rest. Further, an yearly risk assessment just on the data in question should be done to make sure the mitigation meet the need. The cloud supplier likewise needs an approach that encourages into the security episode strategy to manage any information spillages that may happen.

G. Abuse of cloud services

The cloud’s incomparable storage capacity has permitted both hackers as well as legal users to host and spread malware, illicit software, and other digital assets. These dangers comprise of sharing of pilfered programming, music, recordings, or books. You can diminish your introduction to chance by persistently checking use and setting procedures for what your workers have in the cloud.

H. Malware injection

Malware infusions are contents or code that is inserted into cloud benefits and carry on as valid instances” and keep running as Software as an service (SaaS) to cloud servers. This implies noxious code could be infused into cloud service and observed as part of the software that is running within the servers of the cloud environment. Once an injection is executed and the cloud starts working with it, attackers can snoop and compromise the integrity of critical information and data.

I. Denial of service attacks

Unlike other types of cyber-attacks, which are usually launched to create a long-term foothold and hijack sensitive information, denial of service attacks do not challenge to breach your security perimeter.

Rather, they attempt to make your servers and site inaccessible to approved users.In a few cases, in any case, DoS is likewise utilized as a cover for different malevolent moves, and to bring down security applications, for example, firewalls.
III. TECHNIQUES TO SECURE DATA IN CLOUD

A. Authentication and Identity

Authentication of users and even of communicating systems is performed by different strategies, however the most widely recognized is cryptography [8]. Validation of clients happens in different routes like as passwords that is known independently, as a security token, or in the shape a measurable quantity like fingerprint. One issue with using traditional identity approaches in a cloud domain is faced when the enterprise utilizes numerous cloud service providers (CSPs)[8]. In such a use case, synchronizing personality data with the enterprise isn't adaptable. Different issues emerge with traditional identity approaches while moving framework toward a cloud-based arrangement.

B. Data Encryption

On the off chance that you are intending to store delicate data on an expansive information store then you have to utilize information encryption strategies. Having passwords and firewalls is great, yet individuals can sidestep them to get to your information. At the point when information is scrambled it is in a shape that can't be perused without an encryption key. The information is absolutely useless to intruder. It is a strategy of interpretation of information into encrypted code. In the event that you need to peruse the encoded information, you ought to have the secret key or secret key that is additionally called encryption key.

C. Information integrity and Privacy

Cloud computing provides data and resources to valid users. Resources can be accessed through web browsers and can also be accessed by malicious attackers [2]. A helpful answer for the issue of data honesty is to give shared trust amongst supplier and client. Another arrangement can be giving appropriate confirmation, approval and bookkeeping controls so the way toward getting to data ought to experience different multi levels of checking to guarantee approved utilization of assets [2]. Some secured access mechanisms should be provided like RSA certificates, SSH based tunnels.

D. Availability of Information (SLA)

Non accessibility of information or data is a major issue regarding cloud computing services. Service Level agreement is utilized to give the data about whether the system assets are accessible for clients or not. It is a trust bond amongst customer and supplier [2]..An approach to give accessibility of resources is to have a backup plan for local resources and in addition for most significant data. This enables the user to have the information about the resources even after their unavailability.

E. Secure Information Management

It is a strategy of data security for an accumulation of information into central repository. It is involved operators running on frameworks that are to be checked and afterward sends data to a server that is called “Security Console”. The security console is overseen by administrator who is an individual who surveys the data and takes activities in response to any alerts. As the cloud user base, dependency stack increase, the cloud security mechanisms to solve security issues also increase, this makes cloud security administration significantly more convoluted. It is also called as a Log Management. Cloud providers additionally give some security benchmarks like PCI DSS, SAS 70[2]. Information Security Management Maturity is another model of Information Security Management System.

F. Malware-injection attack solution

This arrangement creates a number of client virtual machines and stores all of them in a central storage. It utilizes FAT (File Allocation Table) comprises of virtual operating systems[14]. The application that is run by a client can be found in FAT table. Every one of the instances are overseen and planned by Hypervisor. IDT (Interrupt Descriptor Table) is used for integrity checking.

G. Flooding Attack Solution

All the servers in cloud are considered as a fleet of servers. One fleet of server is considered for system type requests, one for memory management and last one for core computation related occupations. All the servers in fleet can communicate with one another. When one of the server is over-burden, another server is brought and utilized as a part of the place of that server and an another server that is called name server has all the record of current conditions of servers and will be utilized to refresh goals and states. Hypervisor can be utilized for overseeing jobs[14]. Hypervisor also do the
authorization and authentication of jobs. An authorized client’s request can be identified by PID. RSA can also be used to encrypt the PID.

IV. CLOUD COMPUTING SECURITY STANDARDS

Standards for security characterize methodology and procedures for executing a security program. To keep up a secure environment, that gives protection and security some particular advances are performed by applying cloud related activities by these standards. A concept called “Defence in Depth” utilized as a part of cloud to give security [3]. This idea has layers of barrier. In this way, if one of the systems fails, overlapping technique can be used to provide security as it has no single point of failure. Traditionally, endpoints have the system to look after security, where get to is controlled by client.

A. Security Assertion Markup Language (SAML)

SAML is essentially utilized as a part of business deals for secure correspondence between online accomplishes. It is a XML based standard utilized for authentication, authorization among the partners. SAML defines three roles: the principal (a user), a service provider (SP) and an identity provider (IDP) [3]. SAML provides queries and responses to specify user attributes authorization and authentication information in XML format. The asking for party is an online webpage that gets security information[11].

B. Open Authentication (OAuth)

It is a technique utilized for interfacing with secured information. It is essentially used to give information access to engineers. Clients can grant access to data to designers and buyers without sharing of their identity[3]. OAuth does not give any security independent from anyone else in truth it relies upon different conventions like SSL to give security.

C. OpenID

OpenID is a single-sign-on (SSO) method. It is a typical login process that enables client to login once and afterward utilize all the participating frameworks [3]. It doesn't founded on central authorization for validation of clients.

D. SSL/TLS

TLS is used to provide secure communication over TCP/IP. TLS works in basically three phases: In first phase, negotiation is done between customers to identify which ciphers are used. In second phase, key exchange algorithm is used for validation [3]. These key exchange algorithms are public key algorithm. The final and third phase involves message encryption and cipher encryption.

V. CONCLUSION

In conclusion, the cloud platform is a recently new platform that has the potential to have a great impact on the world. Cloud Computing provides many benefits to its businesses and users such as scalability, platform independent, low-cost, elasticity, and reliability. For example, some of the benefits that it provides to businesses, is that it reduces operating cost by spending less on maintenance and software upgrades and focus more on the businesses it self. In spite of the fact that there are different security challenges looked by cloud computing however in this paper, we have talked about some of them. The systems to counteract them are likewise given in the paper, they can be utilized to keep up the protected correspondence and evacuate the security issues. As the distributed computing is dynamic and complex, the conventional security arrangements gave by cloud condition don't delineate to its virtualized surroundings. Organizations like Cloud Security Alliance (CSA) and NIST are yet taking a shot at cloud computing security. There are a few norms are additionally determined which can be utilized to keep up secure correspondence and security in a cloud stage the same number of frameworks impart in it and perform operations.

REFERENCES

https://en.wikipedia.org/wiki/Cloud_computing