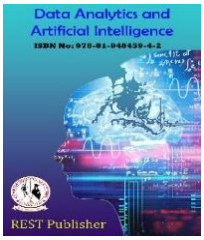
Data Analytics and Artificial Intelligence
Vol: 3(7), 2023
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/daai/



A Server on Cloud Security

***L. Hanupriya**
St. Joseph's College of Arts and Science for Women, Hosur, Tamil Nadu, India.
*Corresponding Author Email: rosehanu06@gmail.com

Abstract: *One of the most fascinating subjects in today's IT industry is cloud computing. The use of the cloud as a computing resource has altered the computing landscape because companies and people have been drawn to its promises of increased reliability, massive scalability, and lower costs. It expands information technology's powers. Cloud computing has become increasingly popular in information technology over the past few years. Concern over the security of information is on the rise as more and more personal and business data is being stored in the cloud. Many organizations, including Microsoft, which is regarded as a giant in the software business, are collaborating to create cloud services.*
Keywords: *Cloud Computing, Cloud Deployment Models, Computing Industry, Distributed Architecture, Server Resource.*

1. INTRODUCTION

Making the transfer from an on hardware to the cloud for your computing needs is the first step in setting your business up for future success. You can access more applications thanks to the cloud, which also makes data more accessible, promotes stronger teamwork, and makes content management simpler. Some users might be hesitant to move their data to the cloud owing to security worries, but a trustworthy cloud service provider (CSP) can allay your fears and protect your data with extremely secure cloud services. Instead of being a novel technology, cloud computing is a new way to deliver information and services using already existing technologies. It enables communication between client-side and server-side services and apps by utilizing the internet infrastructure. Similar to how internet service providers give customers high speed broadband to access the internet, cloud service providers (CSPs) provide cloud platforms for their customers to use and build their web services. Both and ISPs provide services. A layer of abstraction between the computing tools an the underlying low-level architecture is provided by the cloud. Customers simply pay a subscription fee to the cloud service provider, who then gives them access to the infrastructure and resources of the cloud; they do not actually own the physical infrastructure. These hosted services are normally separated into three broad categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

2. CLOUD ARCHITECTURE

The term "cloud security architecture" applies to all the software and hardware components used in cloud platforms to protect data, workloads, and systems. When creating blueprints and layouts for cloud platforms, a strategy for cloud security architecture should be established and incorporated from the ground up.
Five crucial characteristics of cloud computing give it an edge over competing technologies. These characteristics are as follows:
2.1. Multi-tenancy (shared resources): Cloud computing is built on a business model in which resources are shared at the network, host, and application level. This contrasts with earlier computing models, which presupposed dedicated resources dedicated to a single user or owner.
2.2. Massive scalability: Cloud computing enables massive bandwidth and storage area expansion as well as scaling to tens of thousands of systems.
2.3. Elasticity: Users computing capabilities can be quickly increased or decreased as needed, and they can also be released for other purposes when they are no longer needed.

2.4. Pay as you go: Users only pay for the resources and time they truly consume.
Users can self-provision resources like extra systems (processing power, software, and storage), as well as network resources.

3. CLOUD DEPLOYMENT MODELS

Public, private, and hybrid clouds are the three major categories of cloud deployment models**.**

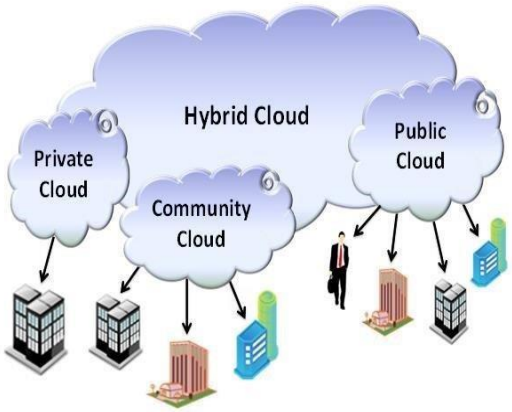


FIGURE 1. Cloud Deployment Models

3.1. Public cloud: The most popular kind of cloud is called a public cloud. Here, numerous users can connect to the internet and use web apps and services. Resources are dynamically provisioned by a third party vendor for each unique customer. This third-party provider handles all security, hosts the cloud for numerous customers across numerous data centers, and provides the necessary hardware and infrastructure for the cloud to function. The customer has no influence over how the cloud is managed or access to information about the available infrastructure.

3.2. Private cloud:
This cloud computing platform is applied in a secure cloud environment and is protected by a firewall that is overseen by the IT department of a specific corporate. Private cloud provides the company more control over their data and only allows authorized users. The physical computers can be hosted either locally or abroad, and they give the private cloud services access to a specific pool of resources. Businesses are better suited to adopt private cloud if they have unforeseen or dynamic needs, crucial management responsibilities, and uptime requirements. Additional security restrictions and bandwidth restrictions that may be present in a public cloud setting are not necessary in private clouds. Cloud companies and customers are in charge.

3.3. Hybrid Cloud:
It is a form of combined cloud computing. It could consist of a mix of two or more cloud servers, such as a private, public, or community cloud, that are connected but separate distinct things. Hybrid clouds are able to transcend provider boundaries and isolation, making it impossible to classify them as either public, private, or community clouds. By assimilating, aggregating, and customizing another cloud package or service, it enables the user to increase both the capacity and the potential. In a hybrid cloud, the resources are either internally controlled or managed by third parties. The task is adapted between the two platforms in accordance with the requirements, switching between the private cloud and the public cloud.

3.4. Community Cloud:
A lot of businesses that are a part of the same community, like banks and trading firms, share the setup in this sort of cloud hosting. There are numerous tenants sharing the multi-tenant arrangement organizations that are part of a group that is concerned about computing in a comparable way. Most of the time, these community members have comparable performance and security worries. The groups' primary goal is to accomplish business-related goals. The community cloud can be hosted publicly or internally, and it can be managed either internally or by third-party providers. Since specific community organizations share the expense, community clouds have the potential to reduce costs. The promise of cloud hosting has been recognized by businesses to excel in everything.

4. SECURITY ISSUES

To varying degrees, almost every enterprise has incorporated cloud computing into its processes. Yet, as a product of this use of the cloud, the business must make sure that its cloud security strategy can fend off the major threats to cloud security.

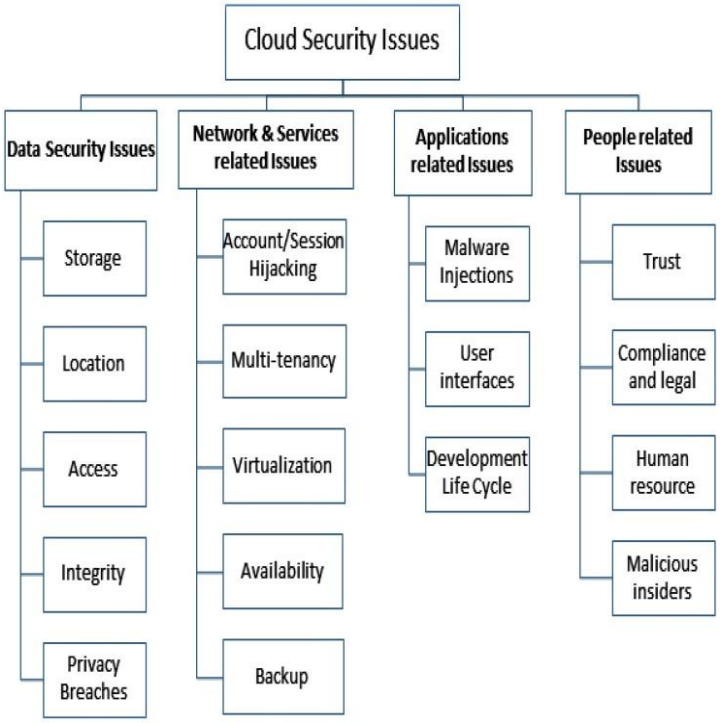


FIGURE 2. Cloud Security issues

In addition to offering customers a variety of services, cloud service
models also divulge data that raises security concerns and increases the risks associated with cloud computing systems. The most potent functionality of a cloud is immediately provided by IaaS, which is found in the bottom layer. IaaS also allows hackers to carry out high-resource attacks like bruteforce cracking. IaaS offers the perfect framework for hackers to start attacks that call for a lot of attacking instances because it supports multiple virtual machines. Another security concern with cloud platforms is data loss. Both external hackers and unauthorized internal employees can readily obtain data in cloud models. Internal staff members have easy access to data, whether on purpose or accidentally.

5. THREATS IN CLOUD COMPUTING

5.1. Broken authentication and compromised passwords: Companies and organizations occasionally run into identity management issues when attempting to give users the permissions necessary for their job roles. When a user leaves the company or a work function changes, they occasionally forget to remove user access. More than 80 million customer data were exposed in the Anthem breach, which was caused by stolen user credentials. Since Anthem didn't use multifactor authentication, everything was lost once the attackers got their hands on the passwords. Many developers have made the error of storing passwords and cryptographic keys in public-facing repositories and embedding them in source code.

5.2. Data breaches:
Cloud environments face many of the same threats as traditional corporate networks, but since a large amount of data is stored on cloud servers, providers have become an attractive target. The severity of the damage tends to depend on the sensitivity of the data that is exposed. Personal financial information grabs the headlines, but breaches involving government information, trade secrets can be more devastating. When a data breach takes

place, a company may be subjected to legal action. Breach investigations and customer notifications can rack up significant costs. Indirect effects may include brand damage and loss of business can impact organizations future for years.

5.3. Hacked interfaces and APIs:

Today every cloud service and application now offers APIs. IT teams use these interfaces and APIs to manage and interact with cloud services, including those that offer cloud provisioning, management and monitoring. The security and availability of cloud services depend on the security of the API. Risk is increased with third parties who rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials. APIs and Weak interfaces may expose organizations to security related issues such as confidentiality, accountability, availability APIs and interfaces are the very much exposed part of the system because they can be accessed from open Internet.

6. SECURITY CHALLENGES OF DEPLOYMENT MODEL

Malicious attacks: Both internal and external sources can pose security risks to companies. 21% of cyber-attacks, according to the 2011 Cyber Security Watch Study, were initiated by insiders. According to 33% of respondents, insider attacks are more expensive and harmful to companies. The majority of insider attacks (63%) and intellectual property theft (32%), respectively, involved unauthorised access to and use of company information. Certain private data can be accessed by malicious users, which can result in data breaches. Injurious assaults by unauthorised users on the victim's IP address and physical server have been demonstrated by Farad Sabah. The malicious intent could be anything from data stealing to retaliation. An insider in a cloud environment has the power to alter, steal, or demolish entire infrastructures. systems that are entirely dependent.

Backup and Storage: The cloud provider should make sure that regular data backups are adopted and that security is fully protected. However, the backup data is typically discovered in an unencrypted format, which can result in data misuse by unauthorised parties. Data copies thus present a number of security risks. An extremely challenging backup and storage issue arises as server virtualization grows. One method to lower backup and offline storage sizes is data deduplication.

7. SECURITY CHALLENGES OF DEPLOYMENT MODELA

Platform-as-a-service (PaaS) security issues: PaaS allows deployment of cloud based applications without the cost of buying and maintaining the underlying hardware and software layers. PaaS depends on a secure and reliable network. PaaS application security constitutes two software layers: Security of the PaaS platform itself and Security of customer applications deployed on a PaaS platform.

Third-party relationships:

Along with providing third-party web services components like mashups, PaaS also provides conventional programming languages. Mashups can incorporate multiple source elements into a unique, cohesive whole. As a result, mashups and PaaS approaches have security problems. Users of PaaS are reliant on the security of both third-party services and web-hosted programming tools.

8. CONCLUSION

A novel idea, cloud computing offers its customers a wide range of advantages. However, it also brings up a few security issues that could limit its application. Organizations can transition to using the cloud more easily if they are aware of the risks that exist in cloud computing. Because it makes use of numerous technologies, cloud computing also carries over their security flaws. Traditional web applications and virtualizations have been considered, but some cloud-based options are either nonexistent or in their infancy. We have discussed security concerns for IaaS, PaaS, and IaaS cloud platforms, each of which has unique security concerns. Storage and networks are the main areas of security worry in cloud computing, as this paper explains. Using virtualization, several people can share a single physical server.

REFERENCES

[1]. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825- 830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[2]. B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009

[3]. National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011.

[4]. Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Security and Privacy. New York: O'Reilly.
[5]. McFedries, P. (2008, August). The Cloud Is The Computer. IEEE Spectrum.
[6]. Mikkilineni, R., & Sarathy, V. (2009). Cloud Computing and the Lessons from the Past. In Proceedings of the 18th IEEE International Workshops onEnabling Technologies:
[7]. Infrastructures for Collaborative Enterprises, Groningen, The Netherlands Garfinkel T, Rosenblum M: When virtual is harder than real: Security challenges in virtual machine based computing environments. In Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. CA, USA: USENIX Association Berkeley;2005:227–229.
[8]. Morsy MA, Grundy J, Müller I: An analysis of the Cloud Computing Security problem. In Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC; 2010.
[9]. Farzad Sabahi, "Cloud Computing Security Threats and Responses", 978-1-61284-486- 2, IEEE, 2011, pp: 245 – 249.
[10]. Intel IT Center, "Preparing your VirtualizedData Center for the Cloud".