SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 10 | October 2024 - Peer Reviewed Journal

SECURITY CONCERNS WITH CLOUD COMPUTING PRACTICES

Kamalakannan Balasubramanian
Leader, Software Engineering @ Cisco Systems Inc
Santa Clara, California - 95054, United States,

Article DOI: https://doi.org/10.36713/epra18580
DOI No: 10.36713/epra18580

ABSTRACT

In order to have more compute and storage facilities, cloud computing is one of the fastest growing sectors with the fastest acceptance and adoption rate. However, as more enterprises migrate to the cloud, data security and plausibility become a big concern for both the organisations migrating to the cloud and the cloud providers themselves. In general, it is the obligation of both suppliers and consumers to collaborate in order to improve the security of deployed models.

KEYWORDS: *Cloud, Computing, bandwidth, storage.*

I. INTRODUCTION

A cloud is a network-accessible organisation that is hidden from users. Cloud computing is a collection of technologies that work together to deliver hosting and storage services through the Internet. Depending on the use cases for a certain individual or organisation, clouds can be defined as public, private, or hybrid cloud.

With the increasing popularity of Total cloud-based systems, cloud operators have been concentrating on their consistency, security, privacy, and cost-effective cloud design. Cloud programme requirements vary greatly depending on the resources that are requested as services. As a result, the sources may also upward thrust to heavy computation sources, large garage sources, large community sources, and so on. In other words, cloud computing is a popular term for delivering hosted artwork over the Internet. It does, however, provide significant benefits to the project; but, as with any new technology, it also has a number of drawbacks. One of the most important topics is the security and privacy of customer information in terms of its location, accessibility, and security. Cloud computing can also be defined as the ability for a community or a remote server to store, manipulate, and manage data over the internet.

II. HEURISTIC SEARCH METHOD

Customers and businesses can use programmes on any computer connected to the Internet thanks to cloud computing. Without any previous connections or access to private files, directly. Users simply need to use the information and resources and pay for the service, which saves time and money by avoiding the usage of third parties.

Businesses provide cloud computing services, which users can access via the Internet.

III. DEPLOYMENT OF CLOUD SERVICES

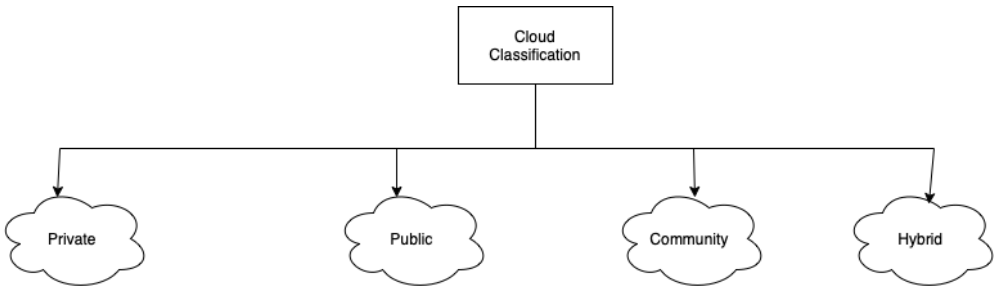
Private cloud, public cloud, hybrid cloud, and community cloud are the four types of cloud readiness models.

- **Private Cloud:** This cloud computing is comparable to public cloud computing in that it incorporates "scalability" and "reliability." The fundamental distinction between a public cloud and a private cloud is that a private cloud is created particularly for a single company.
- **Public cloud:** In terms of "scalability" and "reliability," this cloud computing is similar to public cloud computing. The primary difference between a public and private cloud is that a private cloud is designed specifically for a single enterprise.
- **Hybrid cloud:** This is essentially a collaboration between the public and private cloud systems.
- **Community cloud:** a cloud that is shared by several organisations and is set up to meet their specific needs. The framework may be owned and operated by the businesses themselves or by the cloud service provider.
- Three primary models characterise the nature of the services that cloud computing providers give to their cloud customers: 1. Software as a Service (SaaS): SaaS, often known as "on-demand software," is a cloud computing layer that allows users to access information and applications via the Internet rather than locally. Customers can use computers, desktops, mobile phones, browsers, and other devices to access these services.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 10 | October 2024 - Peer Reviewed Journal

- Three primary models characterise the nature of the services that cloud computing providers give to their cloud customers: 1. Software as a Service (SaaS): SaaS, often known as "on-demand software," is a cloud computing layer that allows users to access information and applications via the Internet rather than locally. Customers can use computers, desktops, mobile phones, browsers, and other devices to access these services.

The Various models are depicted in the diagram below.



IV. SECURITY IN CLOUDS

Gartner, a research and consultancy firm based in the United States, has stated that cloud computing for provider-enabled programmes will take another seven years to attain commercial maturity. Scalability, interoperability, shared environment, and security are just a few of the issues it has faced thus far, not to mention other business-related issues. There's no arguing that cloud resources are virtualized; outstanding cloud provider customers share the same infrastructure and platform for developing software and storing data. Structure set, asset alienation, and information segregation are three key hobbies. Any unauthorised and violent access to a cloud provider's sensitive information might also compromise its integrity, confidentiality, and privacy.

A. Cloud Threats

Some of the threats have been studied over time, and it has been discovered that theft and illegal access have compromised enormous amounts of data. Losses, combinations, IT incidents, and incorrect disposal made up the rest of the security threats.

B. Technical Issues

- **Security**: "How can information be locked safely?" is how security is defined. The fact that sensitive business data would be stored outside the company's firewall raises serious issues. If adequate precautions are not followed, a great deal of very sensitive information could be made public. Even if only one site is hacked, hacking and other assaults on cloud infrastructure will affect several clients. Using security apps, encrypted data file schemes, data loss software, and acquiring security hardware to track out-of-the-way conduct across servers helps reduce these dangers.
- **Distributed-Responsibilities**: Users must check before uploading sensitive data to cloud storage, which is the biggest security risk. You should also use 32-bit encryption as part of your security procedures. This is critical because you may safeguard your data on the cloud by encrypting it before storing it.
- **Fault tolerance and failure recovery:** The data center's sole function is to process massive amounts of data every day. Cloud services may experience data loss if the cloud system fails. Breakdown can be caused by a lack of power, a lack of room, or a failure of the primary system.

V. CHALLENGES FACED IN CLOUD COMPUTING

These are some of the security challenges and their knowledge is needed for mitigation purposes.

Privileged User Access: To avoid data breaches, clients who access data outside the business must get authorization or purchase membership.

Data Location: The client should be completely unaware of the location of data storage and distribution.

Availability: Even if the company's service is now unavailable, the data should be available elsewhere. Always-on software availability is the term for this situation.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 10 | October 2024 - Peer Reviewed Journal

Regulatory Compliance: Even if the company's offer is temporarily unavailable, the data should be available everywhere. Always-on software availability is the term for this.

Recovery: In the event that data is lost due to man-made or natural disasters, the provider must be able to deliver backup data to the customer in a timely manner.

VI. SECURITY RISKS IN CLOUD COMPUTING

Cloud computing allows you to access an organization's data and information. Hackers and attackers have discovered a number of ways to gain access to this data, including:

IP Spoofing: The examination of data transmitted via a network is known as IP spoofing. The attacker manipulates the data as it is transferred over the network. The procedure is carried out in such a way that the trusted system's IP address is adjusted, then the packet information is edited and forwarded to the receiving system.

DDOS attack: The server becomes perplexed, unsure how to handle all of these requests, and authenticated data is leaked.

Insecure Interface: Customers can use interfaces to comply with cloud-based internal software. These APIs are used for data administration, identity management, monitoring services, and other cloud-based operations. If the interface is unsecure, data theft is quite straightforward.

Data Loss or Leakage: When data is sent from the host to the client, two procedures take place. The data is first stored in faraway locations, and then it is transported from one run mode to a plethora of others. As a result, any modifications you make now will lead to data loss or leakage.

Malware attack on VM: Unwanted VM-based malware or toolkits used to obfuscate information transferred to the server can jeopardise cloud security. When data is transferred from the server to the client, the same thing can happen. Data such as registry information, system logs, and security programme details are also stored by these viruses or malware. The relationship between these risks is depicted in this flow chart.

He concludes, however, that the loss of control, invalid storage, access control, and data limits that hackers, crackers, and many security researchers cause are due to a lack of control, invalid storage, access control, and data restrictions. Cloud computing is insecure, and various efforts have been taken to lessen such dangers throughout time.

Some attacks are illustrated in below figure [figure2]

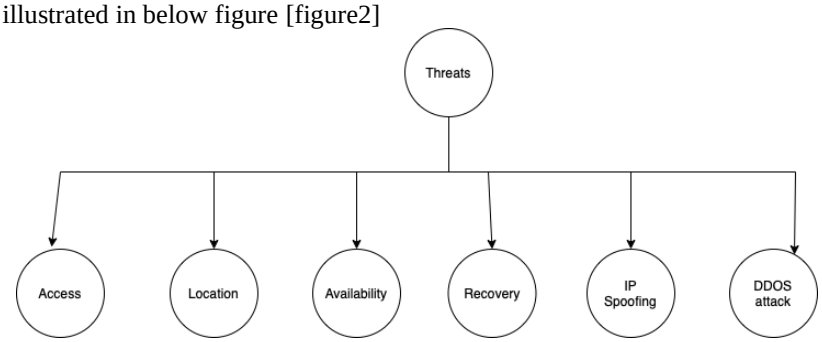


Figure 2: Cloud Security Treat

VII. CONCLUSION

Cloud computing is a fantastic technology that is rapidly gaining popularity. It's a technology that's growing in popularity, with applications in fields including testing and development, big data analytics, and file storage. Although cloud computing and its services are new, many new businesses are adopting them, yet there are always concerns of data breaches. Because of the increased network dependency, firms that use cloud services have more chances for data breaches than traditional organisations. Malware injection is also a major issue in the cloud. An attacker can easily steal important organisational data as a result of this. Those seeking competitiveness in today's economy can gain from cloud companies. The fact that sensitive data is shared while businesses share data is the biggest and most worrisome fear about cloud computing, and the potential for data breaches and data loss is apparent. As a result, all businesses must establish trustworthy security measures in order to protect their

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 10 | October 2024 - Peer Reviewed Journal

consumers' data. Firewalls and intrusion prevention systems are available in many clouds, but they are not suited to your individual system.

VIII. REFERENCES

1. *Azura Che Soh, Mohd Khair Hassan and Li Hong Fey 2004. "Intelligent movement control uor robots using uuzzy logic", Conuerence Artiuicial Intelligence in Engineering and Technology (ICAET-2004), Sabah, Malaysia.*
2. *Farzad Sabahi "Cloud Computing Security threats and Responses", 2011 IEEE 3rd International Conuerence on Communication Soutware and Network (ICCSN), pp. 245-249, May 2011.*
3. *Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conuerence on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ ICCSEE.2012.193*
4. *Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, V. (2010). Security Issues uor Cloud Computing. International Journal ou Inuormation Security and Privacy, 4(2), 39-51. doi: 10.4018/ jisp.2010040103*
5. *Kuyoro, S.O., Ibikunle, F. and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal ou Computer Networks, 3(5), 247-255.*
6. *Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud urom DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding ou the 2010 Second International Conuerence on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.*
7. *V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing " Global Journal ou Computer Science and Technology, Volume 11, Issue 11, July 2011.*
8. *Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal ou Security and Its Application, 6(4), 25-32.*
9. *Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated [2] A. C. Nearchou, "Adaptive navigation ou autonomous vehicles using evolutionary algorithms," Artiuicial Intelligence in Engineering, vol.13, 1999, pp. 159-173. 259.*
10. *J. C. Latombe, Robot Motion Planning, Norwell, MA: Kluwer, 1991.*
11. *Fuzzy Logic Reasoning to Control Mobile Robot on Pre-deuined Strip Path.*
12. *Satveer Kaur and Amanpreet Singh "The concept ou Cloud Computing and Issues regarding its Privacy and Security" International Journal ou Engineering Research & Technology (IJERT), Vol 1 Issue 3, May 2012.*
13. *Hashizume et al. (2013). An analysis ou security issues uor cloud computing. Journal ou Internet Services and Applications, 4(5), 1-13.*