



REVIEW ON SECURITY IN CLOUD SERVICES

Rashmi P. Dagde
Assistance Professor
Computer Science and Engineering
Priyadarshini Bhagwati College of
Engineering
Nagpur, India
rashmidagde24@gmail.com

Nayan P. Mungole
Research Scholar
Computer Science and Engineering
Priyadarshini Bhagwati College of
Engineering
Nagpur, India
nayanmungole160802@gmail.com

Suraj B. Chaudhari
Research Scholar
Computer Science and Engineering
Priyadarshini Bhagwati College of
Engineering
Nagpur, India
chaudharisuraj2002@gmail.com

Shreya N. Thaware
Research Scholar
Computer Science and Engineering
Priyadarshini Bhagwati College of
Engineering
Nagpur, India
shreyathaware9@gmail.com

Abstract: Cloud computing is one of the most used techniques to store the data for the large amount. Over these years it has been attracted so many users towards it because the number of benefits it has. If we talk about its benefits, it will attract you also. It has High Availability, High security (means an ability to store and secure the data at the same time), Transparency of the data to the user, Flexibility, reliability, lower IT cost. Not just this it also gives the assurance and guaranty to the users that whatever happens in any situation, users' data will always be confidential to the unauthorized access. Also, it provides MFA i.e., Multifactor authentication which means there are two ways to authenticate the data. Also, the cloud has no. of services that will blow your mind... Like PaaS (Platform as a services), SaaS (Software as a services), IaaS (Infrastructure as a services). All these services help cloud to secure the data from malfunctioning.

Index Terms: Cloud computing, Security Challenges, Authentication, Authorization, Cloud Models (SAAS, PAAS, IAAS), Cloud Security Techniques

I. INTRODUCTION

Further, the more widespread use of server virtualization has been, a new way has formed for the information technology industry to deliver and spread the complex services we collectively call as cloud. Cloud represents one of the most significant trends in the world of information technology today. Using cloud services is a very attractive option for many organizations to reduce their costs associated with running their own infrastructure. A big plus is certainly reduction in time required to build it. This allows the cloud model on which it is based to shine. The essence of cloud services is their great flexibility. Customers can use computing resources and adapt the use of paid resources according to their needs. The cloud provides a facility to store and access the data from different regions through an internet connectivity. With a cloud server, users can easily store their local data on a remote server. According to Gartner who leads in cloud, cloud computing is among the 10 most relevant technology today. Individuals and organizations are use it to transfer their files and data. Cloud computing has gathered the attention on the business community and academic researchers. Its structured has reform information systems and is regard a part of the future driving technology. Cloud computing allows users to overall share information's, services, and resources. The best examples are Google Apps like Gmail, Google pay, where anyone can access their data using applications via a web server without that much attacks on their data. The storage of data in the cloud decreases the cost of hardware and enhance the reliable Ness of storage. Cloud computing provides a shared pool of computing resources, such as storage devices, servers, networks, and services requiring minimal management efforts Meanwhile, it has many disadvantages. For instance, since it is made up of dispute networks, the cloud surrounding is accessible to the same security threats as any network. Its concept developed from the grid and disquiet computing domains used to host websites, mail servers, and web storage.

II. METHODOLOGY:

2.1 Cloud Computing: As we know that “Cloud” refers “Internet” which means to store the data. Cloud always going to require an Internet connection to store and secure that data from malfunctioning that is called as Cloud Computing

2.2 Security Challenges: These are some of the challenges faces by cloud computing in a security which has tremendous impact on the security in terms of a data.

Data is the most powerful tool which has both advantages and disadvantages too. Nowadays everything is online and virtual.

The below diagram showing, what exactly the cloud computing does and what is the purpose of it.

It has included Data Security, Availability, Compliance, Identity and access management where each term performs their own task to secure the data.

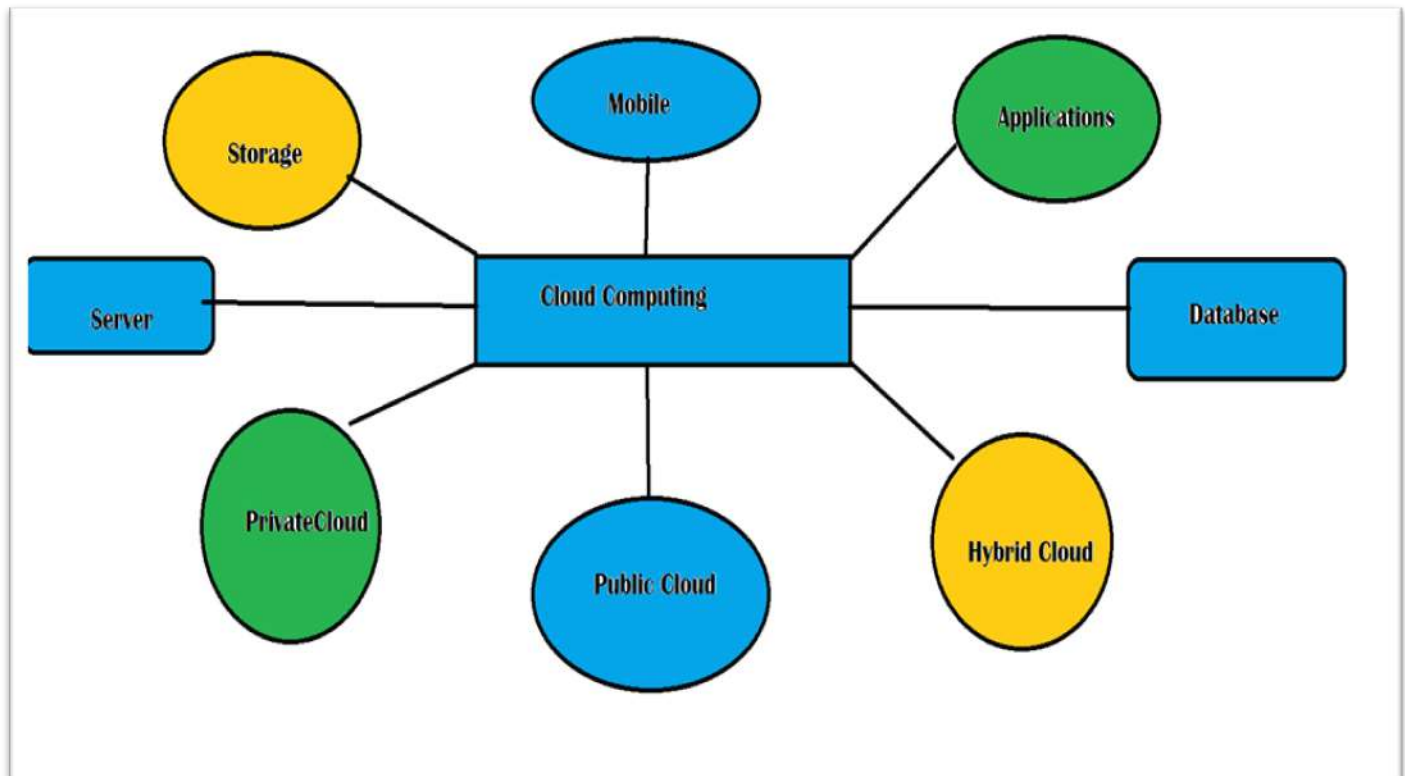


Figure 2.1: Cloud Computing

2.3 Authentication: The name itself saying that it is the most important and weakest part of the cloud computing. It is a Two-way process. There is a term in cloud computing which called as Multifactor Authentication and authentication is the same process. Why it called as a Two-Way process because it is password protected. The data which is provide by the user and store by the cloud is confidential, without Authentication there is high risk that the data can be harm by the attackers. For example, whenever you try to login to your any social media account you have to put your username and password which shows the Two-way process, without that your account will not be access or open.

2.4 Authorization: - It is the Two-factor Authentication process. If a user wants to authorised its account that it has to be authorised. Whenever you are logging for the first time the system asks for the verification that you are the original author or not. You get a verification call through the number or on your mail id you get a message to verify on which you have to clicked after that you can access the data.

2.5 Cloud Models (SAAS, PAAS, IAAS): Cloud computing has Provided various services which are shown below. These are the models of cloud computing used for the security of the data, which are shown below, about whom will get to know more about them.

SaaS (software as a service): It is the service in which the company just develops the software’s for the users nothing else. Software as a Service (SaaS) is a model of cloud computing in which a company only develops the software for the users. The concept of software as a service is based on the ready-to-use format, which means users can directly use the software and apply on the system.

PaaS (Platform as a service): It is specially and primarily used for the developers to implement their own idea of code on software solutions and. The main purpose of this service is to make it easy to used and to create new applications, but also to simplify their production of the deployment along with the maintenance of the software project during runtime.

IaaS (Infrastructure as a service: It is the Hardware as a service which is one of the important layers of the cloud. Basically, it allows the customers to change, transfer and outsource the data from other resources because of that it is called as infrastructure as a service shortly known as “Infra”. It provides some of the services like Computing, Storing the data, Network Load balancing and what not. We can share the data for the huge amount of time and access from web.

2.6 Cloud Security Techniques: As the name suggesting that it will show us what are the techniques to secure the data of the users in the cloud computing using some of the services shown below:

Data Encryption: It is the technique of cloud security which is used to transform the data from its original plain text format to the cipher text that is in the form of unreadable format and all these actions should happened before transforming and store the data to the cloud. That is called as a Data encryption. To encrypt the data, users should have the key called as encrypted key. Its very important to encrypted the data that it will not be visible to other users.

Data Isolation: It is the technique of cloud security which is used to check and ensure the privacy of the user. It separates and disconnected the original data from the network to make it safe after doing this rest of the organisations IT peoples can add impenetrable and unchangeable data, which itself sets a barrier to the harmful events and it will be very hard to find out by the attackers about the original data.

Role based Authentication: Role-based access control, it is the technique which is used to manage the user access to cloud resources. The name role itself gives an idea to us. Cloud security provide role and access of the data according to the individual users within an organisation. According to the ability of work of the model, server or we can say the of the candidate... work will be allocated by the system. That is why it is known as Role-based Authentication.

2.7 Benefits of Cloud Computing:

Security: Many organizations all around the world now belief that Cloud has the highest security compare to any secure organization. The companies like Google used now Cloud and now it is known as Google Cloud where we stored our data in terms of photos, documents ...etc. Security is the most important and vital parameter for any organization which are involved in the Data or to the database, servers. Security is must, if all these roles are fulfilled by any company or organisation, clients will trust those companies to secure their data.

Flexibility: Cloud has the flexible body, which means that we can access over data from any source and any part of the world, which is again one of the biggest advantages of cloud computing for the users. It is very useful benefit of the cloud because we can access our data from any part of world. That means we don't need to always grab our system devices with us. That is why it is very important and useful benefit of the cloud.

Scalability: Cloud computing is the scalable Technology, which means it has the ability to change according to the requirements of the client or user in increasing and decreasing manner which is also another one of the best benefits of cloud computing to the user. Cloud can change its requirements

Cost Saving: Being a user we always try to save our money in every aspect of our life. Even now if we talk about the store our data somewhere with less cost with all services will definitely goes towards it. To even buy the hardware it will not be required that much of the cost. That is why the cloud is cost specific and easy to maintain. Once you enrolled for any course of information of cloud in terms of cloud, it will always and always cost saving which is even a affordable part for us as a user or as a client.

Disaster Recovery: There can be many disasters which can harm over data from the attackers for that reason we should have the back up as a recovery. Cloud computing have Disaster Recovery that during such unexpected situation user's data should be secured and protected. During a situation ship if we caught inside any disaster first will find about the rescue team to help us. That is what the cloud does when such situation happens. And that term is called as the Disaster Recovery. Cloud automatically recovered the data after the disaster viruses in the system.

III. LITERATURE SURVEY

[1] In this paper, they have proposed about the security and privacy of the cloud computing. That how a cloud model helps to secure the data of the user. Cloud computing is the most used technology these days to uplift, secure and store the data. The trend of cloud technology is emerging day by day which means users are attracting towards it and that is why we required more secure network and privacy. Security and privacy have always been a important part when we talked about the data to be secured. Its very important to check the security patterns before investing into any cloud platform.

[2] In this paper, they have proposed that how much a cloud model is important to trust on it. Because of its amazing security benefits for securing the data, users and most importantly clients are believing its security. As the confidentiality of any data is very important and that's what more important for any user. They have told the importance of CCS's and its scalability. They have also concerned about that they have also raised about whether users cloud users can trust on them.

[3] In this paper, they have proposed about cloud computing, what are the security issues in it irrespective of its issues the cloud is dealing. Also, they have talked about the research challenges. Cloud computing is always a sound making technology in the crowd of technical fields. But still its important to talked about its security issues or the challenges and again how cloud fix them. That is what they have talked in this paper which gives brief information about cloud related all security issues.

[4] In this paper, the authors have talked about the systematic literature review on cloud computing. Also, the security of cloud which is use for protecting the data from the unauthorized access from the attackers. They have also talked about the security threats and mitigation strategies. A thread is someone who identifies a single control flow with a logical sequence of that much of instructions. The mitigation implements the identity and access control. That is all about this paper in short.

[5] In this paper, the authors have talked about the enhancing security of health information by using the modular encryption standard in the mobile cloud computing. Before investing in any cloud security, always check about the health information that how it deals with the security threats, privacy of the data with that much of transparency of information only to the client or the user whose information is that. Mobile cloud computing is the technology which always talked about enhancing the health information of the data.

IV. CONCLUSION

A network's security begins with effective protection against external access, and firewalls serve as a critical perimeter defense to achieve this goal. Over the years, firewall systems have evolved from simple packet filtering methods to sophisticated packet inspectors capable of making decisions based on traffic purpose, sources, and destinations. Among the various firewall technologies, dynamic inspection packet methods have proven to be the most effective in protecting network traffic.

However, a firewall system's effectiveness goes beyond its chosen methodology or technology. The best firewall system should also offer robust logging and reporting features. These features enable comprehensive recording of all actions taken by the firewall system and provide valuable insights into any intrusions that may occur within the computer network. By staying informed through detailed logs and reports, network administrators can promptly respond to potential threats and continuously enhance the network's overall security.

Cloud computing makes everything so easy, affordable, cost saving, easy to maintain, provide security and privacy to the data to configure it, which is a great advantage of the cloud. Over these years, because of its benefits, number of peoples are moving towards its technology to save their data for the long period of time.

Lastly, a well-implemented firewall system, equipped with dynamic inspection packet technology and comprehensive logging/reporting capabilities, serves as a strong defense against unauthorized access and potential intrusions, safeguarding the integrity and security of the network.

V. REFERENCES

- [1] Sajid Habib Gill1, Mirza Abdur Razzaq1, Muneer Ahmad2, Fahad M. Almansour3, Ikram Ul Haq4, NZ Jhanjhi5, *, Malik Zaib Alam6 and Mehedi Masud7 "Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study" *Intelligent Automation & Soft Computing*. 10.32604/iasc.2022.016597
- [2] Dan Gonzales, Member, IEEE, Jeremy M. Kaplan, Evan Saltzman, Zev Winkelman, and Dulani Woods "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds" *IEEE TRANSACTIONS ON CLOUD COMPUTING*, VOL. 5, NO. 3, JULY-SEPTEMBER 2017
- [3] moulika bollinadi under graduate student, mgit, hyderabad, telangana, India. vijay kumar damera assistant professor of it, mgit, hyderabad, telangana, India. "Cloud computing: security issues and research challenges" *journal of network communications and emerging technologies (jncet) www.jncet.org* volume 7, issue 11, november (2017)
- [4] seongmo an1, asher leung2, jin b. hong 3, (member, ieee), taehoon eom 1, and jong sou park1 "a systematic literature review on cloud computing security: threats and mitigation strategies" 10.1109/access.2022.3190545, 2022
- [5] maryam shabbir1, ayesha shabbir1, celestine iwendi 2, (senior member, ieee), abdul rehman javed3, muhammad rizwan 1 norbert herencsar 4, (senior member, ieee), and jerry chun-wei lin 5, (senior member, ieee) "enhancing security of health information using modular encryption standard in mobile cloud computing" digital object identifier 10.1109/access.2021.3049564, 2022
- [6] Himanshu Arora, Monika Mehra, Pramod Sharma, Jaisika Kumawat and Jyoti Jangid, "Security Issues On Cloud Computing", *Design Engineering*, pp. 2254-2261, 2021.
- [7] Y. A. Najm, S. Alsamarrae and A. A. Jalal, "Cloud computing security for e-learning during COVID-19 pandemic", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 3, pp. 1610-1618, 2022.
- [8] Mondal Avijit, Subrata Paul, Radha Tamal Goswami and Sayan Nath, "Cloud computing security issues & challenges: A Review", In 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-5, 2020.
- [9] Doshi Riddhi and Vivek Kute, "A review paper on security concerns in cloud computing and proposed security models", In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), pp. 1-4, 2020.
- [10] Balani Zina and Hacer Varol, "Cloud Computing Security Challenges and Threats", In 2020 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-4, 2020.
- [11] Shuanglong Pang, Xiaodan Chen, Desheng Zeng and Cui Shao, "Research on SDN-based Data Center Network Architecture in Cloud Computing Environment", *Electronic Technology*, vol. 525, no. 8, pp. 39-41, 2020.