International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

SURVEY ON SECURITY THREATS AND REMEDIES IN CLOUD COMPUTING

Ms. Mahalakshmi K R[1], Ms Megha H C[2], Ms. Nandini B R[3], Mrs. Hamsaveni M[4]

[1]M. Tech CSE, Dept. of Computer Science &Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
[4]Assistant Professor, Dept. of Computer Science &Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India.

Abstract: Nowadays Cloud computing is an emerging and evolving technology and has become very necessary for computing resources and storing. A huge amount of data is stored inside the cloud by providing high level of fault-tolerance. Cloud computing not only allows users to store the data in the data-centers, also allows to compute resources on-demand. The data inside the cloud can be accessed through the remote servers. Cloud computing serves as internet accessible business model for resource allocation and provides computing infrastructure on a pay-per-use as utilities. Security is the major challenge in cloud computing as the data is being transmitted to the servers via internet. In this paper we have discussed security threats and risks associated with cloud computing, and security concerns in cloud.

INDEX TERMS-Cloud Computing, Security, Threats/risks, and controls in cloud.

INTRODUCTION

Cloud computing is the terminology for communication which provides services by using Internet to provide all resources. It might be networks, servers, storage space, applications and other required services. Any information in the cloud are stored in the remote data servers and can be retrieved and managed using cloud services which are provided by the service providers. Cloud computing is evolving to be widely used these days, and increasing its wage. It's a recent technology that has been exposed and has gained huge importance in the information technology. This paper discusses about the existing deployment models and services of cloud. There are three different deployment models which can be considered, they are Public cloud- these clouds can be accessed by the public through Internet and it is not recommendable. Private cloud- The access to these clouds are forbidden to the public and only authorized people can have access to these clouds. Hybrid clouds- It is the combination of both the public cloud andprivate clouds, and have customized features. The services provided by clouds are: Software-as-a-service (SaaS)- it gives application service to the user, Platform-as-a-Service (PaaS)- It helps the user to install customized applications without any additional tool or software. Infrastructure-as-a-Service (IaaS)- It helps the user to use storage and networks to run applications in local systems. It also discusses the security/confidentiality of cloud computing. The security issues of the clouds needs to be resolved and also clouds will give certain features like data backups to secure or to retrieve the lost data. In this paper we have discussedsecurity threats/risks associated with cloud computing, and security concerns in cloud.

I. DEPLOYMENT MODELS OF CLOUD

1. **PUBLIC CLOUD:** Public clouds works on Internet and is open to all users. The infrastructure used is shared data center and contains all the data of every users [2]. Usersdata is stored in the provider's data center and managed by the service providers. Since it is open to all users it is not recommendable even though it contains some compliancy regulations. Public clouds provide excellent performance as they use shared-resources, but they are vulnerable to various kinds of attacks.

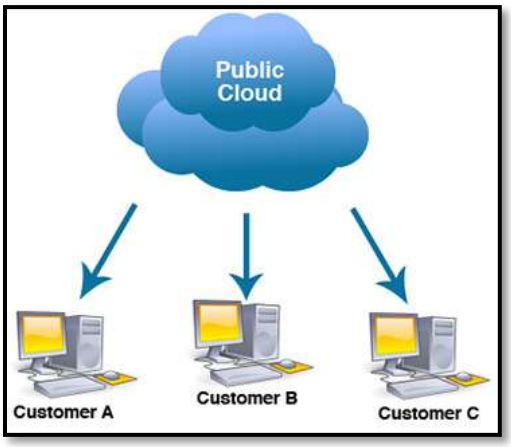

Figure 1: Public Cloud

2. **PRIVATE CLOUD:** In the private cloud data centers are owned by the particular organizations or a company and managed by the

same. It has no access to external users and gives access to authorized people [2]. Private clouds provides more flexibility, scalability, provisioning, automation and monitoring. Increased redundancy, Use of dedicated, private hardware, Decreased provisioning time for new servers.

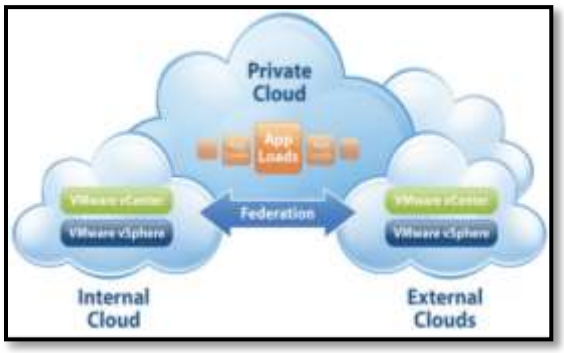

Figure 2: Private Cloud

3. **HYBRID CLOUD:** Hybrid cloud is the combination of multiple clouds i.e., both private cloud and the public cloud, it provides lower cost solutions to issues which might raise during the usage of clouds [2]. It consists of customized features and flexible for users to sort out their feature issues. It provides both private and public environments. Hybrid cloud works well for finance, healthcare, legal, retail industries.

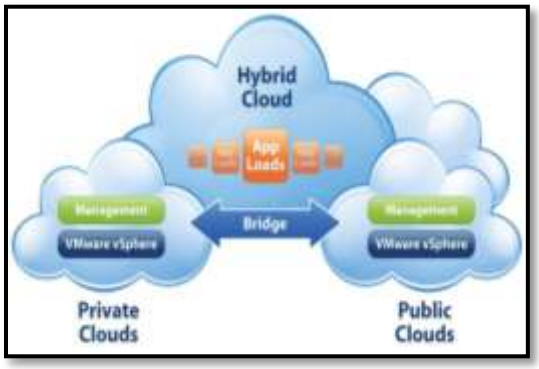

Figure 3: Hybrid Cloud

II. TYPES OF CLOUD SERVICES

a) Software-as-a-Service (SaaS)
The abbreviation of SaaSis Software as a Service. This is the very first layer of cloud and gives the platform for users for installing applications and to use those applications from cloud and does not give the burden of maintenance [3]. It works for the favor of users with user friendly interfaces.

b) Platform-as-a-Service (PaaS)
The abbreviation of PaaS is Platform as a service. It provides freedom to use any applications without downloading any specific platforms to that application. We can use or integrate other applications by using porting. Paas is an effective service to get high productive rate.

c) Infrastructure-as-a-Service (IaaS)
It is the abbreviation of Infrastructure as a service. It provides the storage facility to the user. It makes use of Internet as a business. It mainly focuses on network, storage space, web architecture and deals with managing this architecture [3].

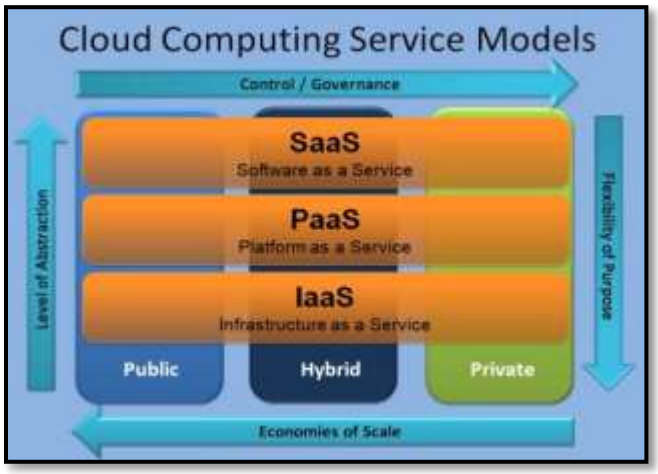

Figure 4. Types of Cloud Services

III. THREATS AND RISKS OF SECURITY

The threats and risks of security areas follows:

1. **Backdoor Channel attacks**
Backdoor channel attack occurs in IaaS platform. when effective user's high permeation is given on the VM's or the Hypervisor level. This kind of attacks may affect the service availability data privacy [4].
2. **Cross-site-scripting attacks:** These kind of attacks are the most powerful attacks of security weakness which commonly found through the web applications. Java scripting language is the widest range scripting languagecommonly used in such attack [4].
3. **Denial-of-Service attacks:** In these attacks, If the users intend to request the service from the server

the service will not be available. It provides the service is not found by displaying 404 error.

4. **Insecure application programming interface:**When the service providers deliver the service to the customers using APIs this type of attack appears, the APIs having encryption with secure authentication, provided with activity monitoring mechanisms secure access control and
5. **Man-in-the-middle attacks:** In this attack the autonomous connection is made between the customer and the service provider, without their knowledge they observe the data and the information for the service.
6. **Metadata spoofing attack:** In this type of attack, The service metadata document is sent to the client system bythe web services providers it contains all the service invocationinformation, such as the message format, security requirements, also the network location. In this case, objective of the attacker is to reengineer the web service metadata descriptions.
7. **Malicious insiders:** This kind of threat happens when there is alack in security concern for how to access the service provider by employees to the virtual properties of the cloud. This threat may be more complex due to employee's privilege in lack of implementing in the cloud system and updated the responsibilities when their behavior or job is changed.
8. **Phishing attack:** This kind of attack affects the user privacy and the exposure of data and information. The users are allowed to access fake web link which is installed in their PCs: that data is exposed by malicious codes.
9. **SQL Injection attacks:** This kind of attack occurs when hackers are trying to attack website database through the website inquiry methods that can deactivate website securityby the code injected inside SQL statements.
10. **Shared technology's vulnerabilities:** This kind of issue is related to cloud computing. It uses the infrastructures same as that is used in the internet shared among cloud customers. Hence, all the problems that are currently in the infrastructure of the internet will be migrated to the cloud.

IV. IMPROVEMENTS/REMEDY & CONTROLS FOR CLOUD

The harmed and hazards are associated with cloud are well documented. Both the one who uses the cloud services and the one who is provided the cloud services has to devised the improvements and controls to understand the risks depends on their evaluation. Here, some of the following more efficient or qualitative and quantitative improvement and control can be considered. They are as follows [5]

1. Extreme part of the encryption

The data belonging to cloud will travels through many geographical places.

2. Examine for diverse activities

It is a part of encryption or end to end encryption technique and it is highly preferable. It is plays a vital role to have proper controls over and improvement to mitigate risks from destructive software passing through diverse activities.

3. Authentication of cloud user

The cloud service facilitator has to take some important precautions to screen the cloud users to prevent important extracted features of cloud being used for diverse attacks.

4. Safe link and APIs

The link is just like interface to cloud and APIs are plays a vital role in implementing robotic, regularity, and to control. The cloud service provider has to ensure that any misused happened.

5. Insider attacks

Cloud providers should take care of safeguard employee and builders, along with build up internal security systems to prevent the misuse.

6. Secure and advantageous resources

In a shared/multi-tenancy model, the hypervisor, orchestration, and monitoring tools has provided by secure and advantageous resources.

7. Business Continuity plans

The process of handling the reporting the response of the organization to any incidents that may cause unavailability of whole or part of a business-critical process is called business continuity plans.

CONCLUSION

As discussed in this paper cloud computing is an evolving technology and has numerous benefits, Consumers are able to use these benefits as per their requirement based on the pay-per-usage facility provided by the cloud.

Security is the major challenge in cloud computing, here in this paper we have discussed some of the features of cloud, deployment models and types of the cloud. Also made a survey of different kinds of threats and risks of security and the improvements remedies and controls of cloud

REFERENCES

[1]. Kowsalyadevi Prakash, "A Survey On Security And Privacy In Cloud Computing" in: 2013 International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 2, February- 2013

[2]. Srijita Basu,Arjun Bardhan, Koyal Gupta,Payel Saha, Mahasweta Pal,Manjima Bose, Kaushik Basu,Saunak Chaudhury, Pritika Sarkar, "Cloud Computing Security Challenges & Solutions-A Survey", in: January 2018,IEEE journal.

[3]. Wg Cdr Nimit Kaura, Lt Col Abhishek Lal, "Survey paper on Cloud Computing Security", in: 2017 IEEE international conference on innovations in information, Embedded and communication systems(ICIECS).

[4].Hussam Alddin S. Ahmed, Mohammed Hasan Ali, Laith M. Kadhum, Mohamad Fadli Bin Zolkipli, Yazan A. Alsariera,"A Review of Challenges and Security Risks of Cloud Computing",in: 2017, Vol. 9 No. 1-2.

[5].Gururaj Ramachandra,, Mohsin Iftikhar, Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing" in: 2017 3rd International Workshop on Cyber Security and Digital Investigation.

[6]. P. Ravi Kumara, P. Herbert Rajb, P. Jelcianac, "Exploring Data Security Issues and Solutions in Cloud Computing", in:2017 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India.

[7].Sabiyyah Sabir, "Security Issues in Cloud Computing and their Solutions: A Review", in: 2018 (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 11.

[8]. Abdulaziz Alshammari*, Suaiman Alhaidari*, Ali Alharbi*, Mohamed Zohdy, "Security Threats and Challenges in Cloud Computing", in: 2017 IEEE 4th International conference on Cyber Security and Cloud Computing.

[9]. Andrey N. Rukavitsyn, Konstantin A. Borisenko,Ivan I. Holod, Andrey V. Shorov, "The Method of Ensuring Confidentiality and Integrity Data in Cloud Computing", 2017 IEEE.

[10]. Ravichandiran C, "Data Security Challenges ans its Solutions for cloud computing", IRACST, IJACEA, ISSN:2319-281X, Vol. 3, No.6, in: December 2014.

[11].Gurjeet Singh, Dr. Mohita Garg, "Data Security In Cloud Computing: A Review", in: 2018 International Journal Of Computers & Technology,Volume: 17 Issue: 02.