Application of security in cloud computing

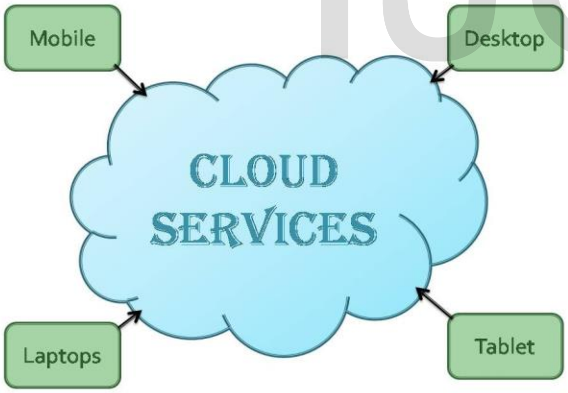
Rashmita Rai, Deepesh Jagadale

Abstract— In today's world, cloud computing has become a prime part of any small and large scale industry. Nowadays, cloud computing is taken into account as a service just like water or electricity is considered as service. A cloud consumer uses different resources such as storage, application, network, etc whenever they need it, without being concerned about the underlying architecture. And users only pay for the resources they need and scale those resources as per their demand. Though cloud provides flexibility in on demand resource availability, it faces some problems in security. And within the future, these problems raised can lead to companies not taking advantage of the cloud-based solutions. This paper provides a literature review on implementing security in cloud environment.

Index Terms: Cloud Computing, Cloud services, IaaS, PaaS, SaaS, Security, Security Issues.

1 Introduction

The Internet has played an important part in the development of different technologies. And one of the popular and discussed technology is Cloud Computing. In the modern world, Cloud Computing has become a trending topic within the organization. A service provided by the service provider can be considered as cloud computing. Cloud computing is the delivery of service to the user over a network typically the Internet. Cloud services can be accessed through different platforms such as mobile, laptop, etc.These services reside within a cloud network. The user does not need to be aware or worry about how the cloud is maintained or how the provider will provide the service. Rather, the user just needs to worry about whether he has proper Internet connectivity or not. The firms do not need to have their own data centers .Nor they have to worry about the costs of the hardware or software, its management, maintenance, storage or power supplies. Enterprises can quickly start-up their business and scale up their business easily using cloud computing. With all these benefits, the cloud also has some downfalls, security being the major one. Because of this disadvantage, companies cannot fully use the functionalities provided by the cloud. To reduce this disadvantage research has been made which will be discussed further in this paper.



2. Cloud service models

According NIST [1], Cloud computing has three service models namely:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Service as a Service (SaaS)

2.1 Infrastructure as a Service

IaaS users are provided with virtualized hardware and storage on which they can build their infrastructure. IaaS provides single hardware to many users. It provides the consumers with full administrative level control. Users can use these r esources to build a platform with the choice of their operating system according to the needs. In Iaas, users have access to server, storage and operating systems. Yet, they cannot access or control the underlying cloud infrastructure. [2].

- *Rashmita Rai is currently pursuing masters degree program in Information Technology in Mumbai University, India, PH-919819234469. E-mail: rrai2550@gmail.com*
- *Deepesh Jagadale is currently a head of depatment in PHCASC, Rasayan, India, PH-9028609874. E-mail: djagdale@mes.ac.in*

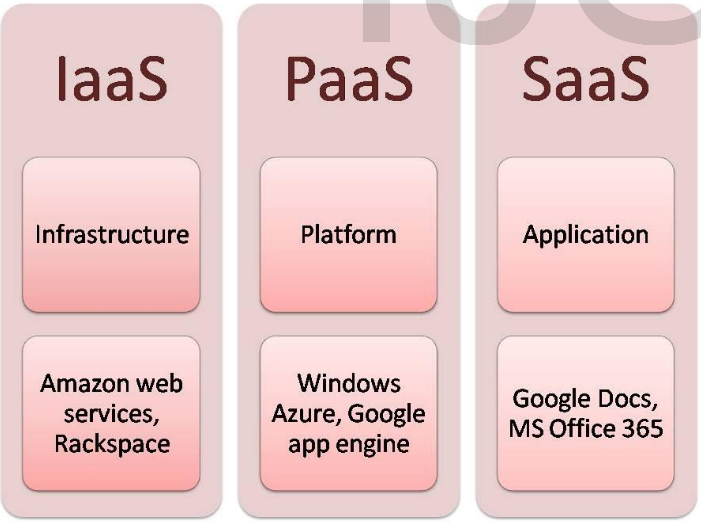
2.2 Platform as a Service

In PaaS, the cloud service provider provides a development platform to the users. The users can easily build their application through a virtual development platform via the Internet without the requirement of any software tools in their computers. The users can then easily distribute and deploy the applications made by them to the cloud. Cloud even provides operating systems or even imitates types of hardware.

2.3 Software as a Service

SaaS has been the most known service model in cloud environment. Typically, a provider delivers the software application needed by the user through the Internet. In SaaS model, the service provider gives access to the user to a single copy of the application that they have specifically created for distribution. This is done using a licensing model in which each application may have a license which is given to a user or an organization. Then the user is able to access the application through an Internet device.

Figure 2 shows the service models in a cloud.


IaaS
Infrastructure
Amazon web services, Rackspace
PaaS
Platform
Windows Azure, Google app engine
SaaS
Application
Google Docs, MS Office 365

3 Literature Review

Different types of techniques are available in cloud security. We will be discussing some of the research work done in cloud security in last ten years.

In 2010, S Subashini and V Kavitha[3], wrote a survey paper. This paper proposes a survey of different security problems that pose a risk to the cloud. The framework that they have showed provides data security by storing and accessing the data based metadata. And if any data is destroyed it can easily be retrieved. Each part of the framework in "security as a service" is provided for practical applications by providers of security as a layer or multiple layers of required applications.
In 2011, V. Krishna Reddy and Dr. L.S.S. Reddy [4] have studied the security problems at different levels of the architecture of cloud computing services. Security of customer-related data is an essential need for services which is provided by each model of cloud computing. They have studied matters of ongoing security software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a Service (IaaS).This paper focuses on the use of cloud services and security for working cross-domain Internet connected.
In 2012 Punyada M. Deshmukh et. al. [5] wrote a paper. In this paper, they have proposed a system which ensures the data storage security using a distributed scheme. A set of Master servers are used which are responsible for processing the users requests. File chunking operation is performed in order to store replicas of file at Slave server providing backup for file recovery. Unlike the previously proposed systems, efficient and dynamic data operations are performed by users. This efficiency is achieved by imparting the data blocks for different users. The functionality is extended to the Android users and the chatting application is included to add ease and comfort to the working environment of users.
In 2013, Sajjad Hashemi[6] published a paper. In this paper he attempted to review and highlight security challenges particularly the security of data storage in cloud environment. He also provides some offers to enhance the security of data storage in cloud computing and by using these opinions one can overcome the problems.
In 2014, Swarnalata Bollavarapu and Bharat Gupta[7] proposes the study of algorithms used for data storage security in the cloud and desktops. Theyhave also discussed encryption and

decryption techniques such as RSA and RC4 to reduce the security problems.

In 2015, Karun Handa[8] et. al. describes that since the resources are easily in cloud computing anyone can access the data using the web. But this advantage comes at a cost. Firstly, the data is uploaded unsecurely which has a high risk of being hacked by some malicious people. Secondly, the data saved at remote servers is under the surveillance of unknown people who can do anything with our data. So, these data security risks are causing a hindrance in the development of the field of cloud computing. Thus, this paper has designed a scheme that can help, solve this issue.

In 2016 Nidal Hassan Hussein[9] et. al. wrote a paper which has a comprehensive survey of existing literature for cloud computing security challenges and solutions is presented. At the end of this paper the authors propose a model for cloud computing security.

Ashok Deokar (2017)[10] discussed the security risks and concerns in cloud computing. This paper also shows how we secure the cloud security, privacy and reliability when a third party is processing sensitive data.He also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management.

D. Hyseni, A. Luma, B. Selimi and B.Cico (2018)[11] have proposed a new approach to security that is controlled by the IT Security Specialist (ITSS) of the company/organization. The approach is based on multiple strategies of file encryption, partitioning and distribution among multiple storage providers, resulting in increased confidentiality since a supposed attacker will need to first obtain parts of a file from different storage providers, know how to combine them, before any decryption attempt.

Yoshita Sharma, Himanshu Gupta and Sunil Khatri(2019) [12] proposes the use of multiple encryption technique outlines the importance of data security and privacy protection. Also, what nature of attacks and issues might arise that may corrupt the data; therefore, it is essential to apply effective encryption methods to increase data security.

4 CLOUD COMPUTING SECURITY

Cloud computing provides services, applications and storage to the users through the providers. Firms use these services in a variety of different deployment models and service models. When they adopt the cloud computing technology, security is one of the critical issues.

Cloud computing security or Cloud security is defined as a set of policies, technologies and controls used to protect or secure data, services and application of cloud computing. Protection ensures that the cloud infrastructure, applications and data is enclosed from the threats.

5 CLOUD SECURITY THREATS

The top security threats in cloud computing are [13]:

5.1 Data Breaches

Data Breach or leak is the most known security concern. It involves unauthorized or illegal viewing, copying or transmiting of data by the hackers.

A breach of security may lead to alteration, loss or destruction of data and can even give access to personal data or information.

5.2 Denial of Service (DOS)

DOS is one of the serious attacks in cloud environment. Denial of service is a cyber attack in which the attackers try to make the resources unavailable to the users by overwhelming the network with unwanted traffic.

5.3 Cryptojacking

Cryptojacking is an emerging cloud security threat. It hides on the user’s computing resources to process the transaction of cryptocurrency. The system slows down since it increases the CPU load.

5.4 Account Hijacking

Account or service hijacking remains to be a serious threat. It is a process in which a person’s or an organization’s account is stolen or hijacked. The stolen account’s information is then used by the attacker to malicious or unauthorized activity.

5.4 Insecure APIs

Even if our system is safe, there are third party services which can introduce to additional cloud security risks. APIs are the intial entry points of the attackers. IoT technologies are mostly considered as a threat to data privacy. API vulnerabilities are not always easy to spot and require specialised technology for detection and prevention.

4 Conclusion

Nowadays, cloud has become a real buzzword. Cloud computing is a virtualized pool of resources which includes storage, service, network, development tools and application. Almost all the online business and applications like Flipkart, Google apps execute in cloud. Cloud provides the resources which a user needs at any time. Security has been a basic concern in cloud computing. Since the volume of the public cloud is increasing rapidly, there is a greater risk of cloud security threats. We have discussed the literature review of different cloud security models, the challenges of cloud and how we can overcome them.

References

[1] P. Mell and T. Grance, “The NIST definition of cloud computing (draft),” NIST special publication, vol. 800, no. 145, p. 7, 2011.

[2] Q.Shallal,Y.Tamandani and M. Bokhari, Cloud Computing service models:A Comparative study (2016)

[3] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, Network and Computer Applications, Elsevier, Vol. 34

[4] V. Krishna Reddy, Dr. L.S.S. Reddy, “Security Architecture of Cloud Computing”, International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1

[5] Punyada M. Deshmukh, Achyut S. Gughane, Priyanka L. Hasija, Supriya P. Katpale, “Maintaining File Storage Security in Cloud Computing”, International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 10, October 2012.

[6] Sajjad Hashemi, “Data Storage Security Challenges in Cloud Computing”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.

[7] Swarnalata Bollavarapu and Bharat Gupta, “Data Security in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014

[8] Karun Handa, Uma Singh, “Data Security in Cloud Computing using Encryption and Steganography”, International Journal of Computer Science Mobile Computing, IJCSMC, Vol. 4, Issue. 5, May 2015, pg.786 – 791.

[9] Nidal Hassan Hussein, Ahmed Khalid, “A survey of Cloud Computing Security challenges and solutions”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016

[10] Ashok Deokar," Cloud Computing Security Issues, Challenges and Solution", International Journal of Innovative Research in Computer and Communication Engineering, Vol.5, Issue.2, February 2017.

[11] Dhuratë Hyseni, Besnik Selimi, Artan Luma, Betim Cico, " The Proposed Model to Increase Security of Sensitive Data in Cloud Computing" , International Journal of Advanced Computer Science and Applications, Vol.9, No. 2, 2018.

[12] Yoshita Sharma, Himanshu Gupta and Sunil Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing", IEEE,

[13] https://easternpeak.com/blog/the-top-cloud-security-threats-for-your-business-in-2019-and-how-to-avoid-them/