International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X

Security Concerns of Cloud

PG Scholar Mamatha R
Department of MCA
Dayananda Sagar College of Engineering
Bangalore, India
mamathargowda1996@gmail.com

Asst. Prof. Mahendra Kumar B
Department of MCA
Dayananda Sagar College of Engineering
Bangalore, India
mahendra-mcavtu@dayanandasagar.edu

Abstract **- Cloud Computing is the practice of using a network of remote servers hosted on the internet to process, manage and store data rather than a local server or a personal computer. Or cloud computing could be the method for delivering information technology service is where resources are obtained from the internet through web based tools as application. Organizations use cloud in a variety of different service models such as Saas, Paas and Iaas which are deployed using deployment models public, private and hybrid**.

Keywords- **Cloud security, Cloud computing security**

I. INTRODUCTION

Cloud Computing is the practice of using a network of remote servers hosted on the internet to process, manage and store data rather than a local server or a personal computer. Or cloud computing could be the method for delivering information technology service is where resources are obtained from the internet through web based tools as application. Organizations use cloud in a variety of different service models such as Saas, Paas and Iaas which are deployed using deployment models public, private and hybrid.

There are a number of security issues associated with cloud computing. The issues fall into two broad categories, security issues faced by cloud providers and security issues faced by the customers.Cloud providers are organizations providing software, platform or infrastructure as a service via the cloud. Cloud providers must ensure that their infrastructure is secure and that their clients data is protected. Meanwhile, the customer must ensure that the provider has taken proper security measures to protect their information.

Due to so many advantages of cloud many organizations are moving towards it so it's very much necessary for cloud providers to provide proper security to users data. Strict privacy and security policies has to be implemented by cloud providers a comprehensive study should be conducted to determine the threats faced by cloud consumers and analyze the privacy and security policy controls to manage these threats.The extensive use of virtualization in implementing cloud infrastructure brings unique security concern for customers using public cloud service. Virtualization alters the relationship between the operating system and underlying hardware. The hardware could include computing, storage or even networking. The layers of virtualization must be properly configured managed and secured. The concerns may include the potential to compromise virtualization software ("hypervisor"). The virtualization layer is managed by a central management console. This Central management console has to be secured.

II. SECURITY ISSUES IN CLOUD COMPUTING

1. Data related security issues

- Data breach- it is an incident in which sensitive data is stolen by an unauthorized individual.
- Data lock in- it is usually called vendor lock in and is a situation in which a customer using a service cannot easily transition to a competitor's product or service that is, user may loose data if they migrate from one vendor to another vendor.
- Data removal- it is the residual representation of data that have been nominally erased or removed in some way.
- Data recovery- it is residual representation of data loss. Data recovery might become difficult in case of server breakdown of failure.

2. Application related security issues

- cloud Malware injection attack- in this kind of attack the attacker focuses on adding a harmful implementation to Cloud Service.
- Cookie poisoning- it is the modification of cookies of a user to gain unauthorized information about user.
- Backdoor and debug option- it is a conventional technique in which system security is bypassed undetectably to access users data on the cloud.
- Hidden field manipulation- attackers modify hidden fields on the web page that yield gathered authorized information about the user.

3. CSP(Content Security Policy) level attacks

- Guest hopping attack- attackers identify two virtual machines hosted on same physical hardware and try to penetrate one machine from another.
- SQL injection- it is a computer attack in which malicious code is embedded in a poorly designed application and then passed to the back in database.
- Malicious insider- it refers to a person or an employee who threatens organizations because he has access to organization system and data.
- Side channel attack - often includes cache attack, attackers monitor cache access to gain access to encrypted data.

4. Network level attacks

- DNS attacks- it includes the domain hijacking and cross-site scripting.
- IP spoofing- in this kind of attack intruder send malicious data to computer with an IP address indicating that the message is coming from a trusted host.
- Man in the middle attack- in this type of attack the attackers monitor communication between two users.
- Network sniffing- here the attacker capture and interpret data flowing through the network and he gains access to all the information going through the network.

III. COUNTER MEASURES

- Enhanced security policies should be introduced and implemented. Security policies like credit card fraud monitoring and block of public Blacklist should be applied to reduce the risk of abuse of cloud.
- Access control mechanisms should be further improved. Only authorized users should be allowed to access their data.
- For data protection various tools should be used like data loss prevention systems, abnormal behavior detectors, encryption tools, etc...
- Security techniques- attacks can be prevented by using file allocation table storing hash values and by conducting integrity tests.

Acknowledgment

The successful completion of paper submission work depends on the co-operation and help of many people, other than those who directly execute the work. I take this opportunity to acknowledge for the help received for valuable assistance and cooperation from many sources.

I express my heartfelt thanks to my mother **Mrs. Mangala Gowri** and father **Mr. Ramakrishne** Gowda for their constant support.

I express my sincere words of gratitude to our Chairman **Dr.Premachandra Sagar** ,for creating an academic environment to brighten our career.

I am deeply in debted to **Dr.C.P.S Prakash,** Principal and **Dr. Samitha Khaiyum,** Professor and Head, Department of MCA. I express my heartfelt thanks to my Guide **Mr. Mahendra kumar B** ,Assistant Professor Department of MCA and **Mrs.Vibha M B** and **Dr. SumaS** Assistant Professor Department of MCA for her constant guidance and devoted support. I also express my heartfelt thanks to friends and well-wishers.

REFERENCES

[1] Akhil Behl"Emerging security challenges in cloud computing"

[2] Farhan Bashir Shaik,Sajjad Haider “Security threats in cloud computing”

[3] Mark D Ryanl"Cloud computing security"