National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Review on Security Issues In Cloud And Introduction To Implementation of Devsecops To Avoid Security Issues In Cloud Computing

Chethan. C, Monisha A V, Reshma . B
Seshadripuram Academy of Business Studies Kengeri Satellite Town Bengaluru, Karnataka, India

ABSTRACT

In today's world Cloud Computing is everywhere. And it can be defined as a huge warehouse of data storage. Cloud computing enables tasks to be assigned to a combination of software and services over a internet. Cloud service vendors hosts the data of the data owners in their servers and the users can access their data through these servers through a Web consoles. Hence Cloud enables the organisation to setup a cost efficient and effective infrastructure virtually and it follows pay as you use basis. The issue here is as the data owners and the severs are two different individuals, Hence proper care to be taken that data is stored in a secured manner with proper encryption. And also the implementation of new technology called DevSecOps will avoid all most all the security issues in cloud.

I. INTRODUCTION

A BRIEF INTRODUCTION ON CLOUD COMPUTING

Cloud computing can be defined as "delivery of computing services (servers, storage, databases, networking, software, analytics, intelligence and more) over the Internet" . Here we typically pay only for cloud services we use, It helps in lowering our operating costs,and helps us to run our infrastructure more efficiently .

Types of cloud :

There are three ways to set up a cloud services :
1): public cloud, 2):private cloud 3): hybrid cloud.
Public cloud : Public clouds are owned and hosted operated by a cloud vendor, which deliver their servers and storage over the Internet.AWS, V cloud , Google cloud and Microsoft Azure is an example of a public cloud. With a public cloud, a complete infrastructure is owned and managed by the cloud provider. You access these things using a web console.

Private cloud
A private cloud refers to cloud computing resources used by a one company . A private cloud can be physically located in the company . Some companies also uses a third-party service vendor to host their cloud. A private cloud is one in which the infrastructure are maintained on a private own network.

Hybrid cloud
This is a combination of both public and private clouds. By allowing data and applications to move between private and public clouds, It gives our business greate freedom and deployment options and helps to secure our infrastructure more efficiently.

Types of cloud computing services:

There are 3 major cloud computing services and they are :

1) : Infrastructure as a service (IaaS),

2) : Platform as a service (PaaS),and 3): Software as a service (SaaS).

Knowing more about these services makes us achieve all the company requirements.

Infrastructure as a service (IaaS)

The most basic service of cloud is IaaS. On a pay as u use basis With IaaS, we can rent IT infrastructure servers and virtual machines (VMs), storage, networks, operating systems from a cloud vendor .

Platform as a service (PaaS)

Platform as a services supply an on demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create a app or website, without worrying about the infrastructure.

Software as a service (SaaS)

Software as a service is a method for delivering software applications over the Internet. With SaaS, cloud providers host and manage the software application and will take care of maintainance of that software like upgrades security of the software etc. Users connect to the application over the Internet using their device.

Following are the benefits of cloud computing:

1. Cost efficient to build a infrastructure
2. Dependable performance
3. Lesser Maintenance issues
4. Regular software updates
5. Improved compatibility between Operating systems
6. Backup and recovery
7. Performance and Scalability
8. Increased storage capacity

Cloud Architecture:

Cloud computing comprises of two components front end and back end. Front end consist client part of cloud computing system. It comprise of interfaces and applications that are required to access the cloud platform.

While back end refers to the cloud itself, it comprises of the resources that are required for cloud computing services. It consists of VMs, servers,storage, security units etc. It is under the control of cloud provider.

Cloud computing distributes the file system that spreads over multiple hard disks and machines. Data is never stored in one place only and in case one unit fails the other will take over automatically. The user disk space is allocated on the distributed file system.

Security problems in Cloud Computing

The major issue that arises in the users mind is about its security.One concern is that cloud vendors themselves may have access to the company's unencrypted data whether it's on disk, in memory or the data that travel over the network.

To provide security for systems, networks and data, cloud computing service providers have joined hands with TCG (Trusted Computing Group) which is non-profit organization which regularly releases a set of guidelines to secure hardware, create self-encrypting drives and improve security. It protects the data from unauthorised access and make sure that data is safe.

As computing involves with different devices like hard disk drives and mobile phones, TCG has extended the security measures to include these devices to make sure that users are safe.

Privacy in Cloud

Privacy present a strong barrier for users to adapt into Cloud Computing systems

There are certain measures which can improve privacy in cloud computing.

1. The administrative staff of the cloud computing service could theoretically monitor the data moving in

memory before it is stored in disk .To keep the confidentiality of a data, administrative and legal controls should prevent this from happening.

2. Here to make sure the data is confidential , cryptographic algorithms and strong authentication process should be used . And encryption of the data is must , here encryption means storing a data in the cloud in such a way that only authorised user can understand and access that particular data. Proper encryption is so powerful that even the cloud service provider will be unable to read the data.

Various security issues in cloud

Security issues while transferring of data to CLOUD

It is the process of transferring data over a medium to one or more computing network. In Cloud environment most of the data is not encrypted in the processing time. To process data for any application that data must be unencrypted. The data theft when the attackers place themselves in the communications path between the users. Here there is the possibility that they can interrupt and change communications to their desired locations.

Security issues in VM's

Virtual Machine (VM) means sharing the resources of single physical computer into various computers. VM's provide agility, flexibility and scalability to the cloud resources by allowing the cloud service providers to copy, move and manipulate their VM's. Keeping this in mind, malicious hackers are finding ways to get their hands on data by breaching the security layers of cloud environments. The cloud computing scenario is not as transparent as it claims to be. The service user has no idea about how the data is processed and stored.And dosent have direct control over the flow of data.

Security issues in Application Programming Interfaces (API)

Customers handle and interact with cloud services through API's. Cloud service Providers must ensure that security is integrated into their service models, while users must be aware of security risks.

DevSecOps Approach to Cloud Security Majority leading firms are striving to deliver high and highly-scalable performance with 24/7 digital services that are built on customized modern architectures. Successful models of modern architectures are being developed on the stack of advanced tiers, technologies and microservices, backed by the market's leading cloud platforms such as AWS, GCP, and Azure.

Above all these advanced services, security continues to be a key concerning factor for the majority of them. Applying DevSecOps for Cloud Security definitely solves the issue. As the surveys show, the majority of firms developing apps on the cloud are inclined towards adopting DevSecOps security tools and processes for improved agility and high reliability.

Adopting DevSecOps principles in Cloud requires an effective strategy and planning involving cultural changes, especially in automating security and configuration of assets in the cloud.

For this, security teams will need to:

• Work in collaboration with Development teams who push code to cloud-based applications, to ensure quality aspect in the production cycle is achieved without affecting the pace of the process

• Coordinate with the Quality Analysis and Development teams in defining qualifier and parameter prerequisites needed for promoting code

Cloud-native machine data analytics platform is also an important requirement to enhance cloud security,

considering the short-term nature of modern applications and limitations associated with the traditional monitoring and security mechanisms.

Adding to the machine data analytics solutions, DevSecOps principles brings you closer to achieving software agility, high reliability and enhanced security through continuous monitoring and keen analyzation of end-to-end tools and processes across the lifecycle.

Implementation of DevSecOps
Separation of development and security are no longer two different aspects.
DevSecOps combined them into a single streamlined process by incorporating security at the level of code, thus ensuring safety of applications and processes at all levels of the process chain.

Five features speak the successful implementation of DevSecOps:

• Mandatory security at every stage
• Thorough Assessment before security
• Security-related changes right at the code level
• Automation of all possible processes
• Continuous monitoring through alerts and dashboards

II. CONCLUSION

In today's world cloud computing is an essential technology where each and every organisation are moving towards cloud but the major fear that is running in users mind is about the security of their data.
Usage of DevSecOps in organisation will reduce the security issues in cloud and also from the clients there should be a proper legal agreement to be done with the cloud provider before the setup of cloud in the organisation . And also an active and efficient team need to be working on encryption of data before storing or transferring the data to the cloud .

III. REFERENCES

[1]. V.Suresh Babu , Maddali M.V.M kumar "An efficient and secure data storage operations in cloud computing". – 2018 IJSRSET volume 4. Themed section engineering and technology
[2]. Supriya D Patil, Komal S Talekar,Reshma R Raskar,Pooja A Chavans –"Attribute based access control in personal health records using cloud computing – 2018 IRJET volume 4.
[3]. Vivek paul , Supriya Panditha – "Cloud computing review" – Mar 2018 IRJET volume 5.
[4]. A Venkatesh , Marrynal S Eastaff – "A Study of data storage issues in cloud computing" – 2018 IJSRCSEIT volume 3.
[5]. M. AlZain, E. Pardede, B. Soh, and J. Thom, "Cloud computing security: From single to multi-clouds," in System Science (HICSS), 2012 45th Hawaii International Conference on, Jan 2012, pp. 5490–5499.
[6]. E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in High Performance Cloud Auditing and Applications. Springer, 2014
[7]. CLOUD COMPUTING: STUDY OF SECURITY ISSUES AND RESEARCH
[8]. CHALLENGES Adnaan Arbaaz Ahmed, Dr.M.I.Thariq Hussan Volume 7, Issue 4,April 2018, ISSN: 2278 – 1323

Cite this article as : Chethan. C, Monisha A V, Reshma . B , "Review on Security Issues In Cloud And Introduction To Implementation of Devsecops To Avoid Security Issues In Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 83-86, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194715