International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 3767 – 3772

A Study of Security Issues and Solutions in Cloud Computing

Anandkumar B[1], P. Devika[2], P. Srinivasa Reddy[3], D.Divya Priya[4]

[1,2,3]*Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad*

Abstract

Cloud computing provides a solution to problem computing. Using all the infrastructure that the cloud vendors provide, cloud users can satisfy all their business needs. These cloud features inspire people to use them. Cloud consumers are largely unaware of the flaws and risks before they accept cloud services. In this paper, we reflect the brief information about cloud infrastructure and models for cloud deployment. In this document, we seek to define the SaaS application security and data protection challenges. The aim of the paper is to provide a SaaS service security perspective and an simple way to solve the problem.

1. INTRODUCTION

The popularity of cloud computing is increasing day by day. It has emerged as a new way for IT capabilities to tackle alternative distributive models. It is a way to deliver IT enabled applications in the form of software, infrastructure and platform. It provides various services to the users on demand and pay as you go policy, accessible everyone, every time, and everywhere.[1]
Cloud Computing can be defined as the custom of using internet hosted remote server network to store, handle, and process data instead of using a local server.

The idea behind cloud computing is that the all the important computations takes place on a remotely maintained server, currently which is not used by any one. The information which is gathered is then processed on cloud servers. The devices that accesses the cloud doesn't have to work hard.
As the cloud hosts the software, platform and databases, it frees up the memory, power of computing of the user's computer. The cloud service provider issues the access credentials to the user using which the user can access his data on the cloud.
Cloud provides various advantages over the present system which includes Scalability, data security, and high performance and so on.

Features of Cloud Computing

Following are some of the important features of cloud computing. [2]

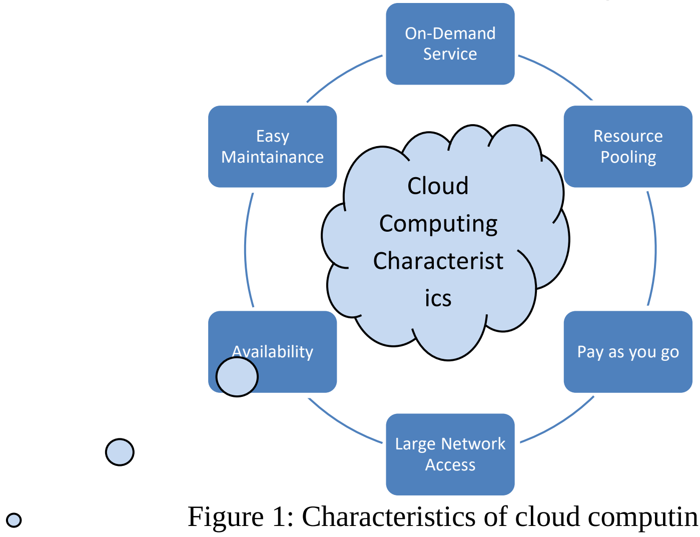

Figure 1: Characteristics of cloud computing

ISSN: 2233 -7857 IJFGCN

On-Demand Service: This means that the cloud service providers allow the vendors to be supplied with cloud resources whenever they are require without human interaction.

Resource Pooling: Resources are shared among multiple customers. Various physical and virtual devices are assigned to customers and reassigned to another customer based on their demand.

Pay as you go: Cloud service providers charge customers only for the resources they use or they service use, without any hidden charges.

Large network access: The user can access the cloud from any corner of the world; the only thing he requires is the internet and a device to access the data.

Availability: The Cloud capabilities can be updated as per use, and can be expanded considerably. It analyzes the usage of storage and enables the customer to buy additional cloud storage for a very limited amount if necessary.

Easy Maintenance: The maintenance of the servers is very easy. Also the downtime of the servers is very small and there are no downtimes except in some situations. The cloud computing also brings up updates very frequent to make it better.

Types of Cloud

Based on the usage, Cloud computing can be broadly classified into three categories.[3]

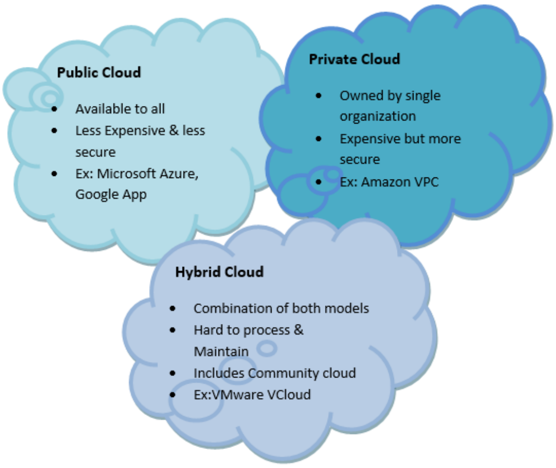
Public Cloud
Available to all
Less Expensive & less secure
Ex: Microsoft Azure, Google App
Private Cloud
Owned by single organization
Expensive but more secure
Ex: Amazon VPC
Hybrid Cloud
Combination of both models
Hard to process & Maintain
Includes Community cloud
Ex:VMware VCloud

Figure 2: Types of Clouds

Public Cloud: They are shared by multiple users on a large scale. Public clouds are hosted by third party service providers. They can be easily accessed using web browsers. Some third party vendors include Amazon Web Services, GoogleCloud, MicrosoftAzure, etc.

Private Cloud: They are maintained by a single organization. The security and flexibility is better in private cloud compared to other cloud types. However, they are can still be hacked and vulnerable to other attacks. Some third party vendors include Amazon VPC.

Hybrid Clouds: It is the combination of both the models. The hybrid cloud is designed to permit seamless interaction between two systems. Some third party vendors include VMware VCloud.

Cloud Computing Services

Cloud Computing services can be broadly classified into three categories. They are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).[4]

Infrastructure as a Service: Here cloud service providers provide customers with the virtualized infrastructure for their businesses. With IaaS, organizations can buy on rent various hardware components for their use such as servers, data center and networking, which has features close to that of an on-site infrastructure.

It is the responsibility of the cloud service provider to build the servers, firewalls, networking and data center. Some of the vendors providing IaaS are AmazonEC2, MicrosoftAzure, GoogleCloud Platform, Go Grid, RackSpace, Digital Ocean, etc.

Platform as a Service: PaaS is built on IaaS. The cloud vendors provide all the hardware and software components required for computing tools, such as middleware and operating systems, needed to build and test applications. The PaaS ecosystem makes sure that cloud users are able to install and host data sets, tools and applications required for their business, besides building and maintaining required hardware.

Some of the vendors providing PaaS are Blue mix, Cloud Bees, salesforce.com, GoogleApp Engine, heroku, Amazon web services, Microsoft Azure, OpenShift, and Oracle cloud.

Software as a Service: It is unique in that it combines IaaS as well as Paas. The cloud computing service provider here provides the entire suite of applications as a pay-per-use platform. SaaS helps users to access applications conveniently over the internet — such as emails.

Some of the vendors providing SaaS are Microsoft Office360, App Dynamics, AdobeCreative Cloud, GoogleG Suite, zoho, Salesforce.com, Marketo, OracleCRM, Pardot Marketing Automation, and SAP Business By Design.

Factors affecting security in cloud computing

There are many main factors that can influence the efficiency of cloud computing, as it is composed of many technologies. Some of them are Network, Operating System, Concurrency control, Virtualization, Transaction management, Resource Management, Memory Management, Database and Load Balancing.[5]

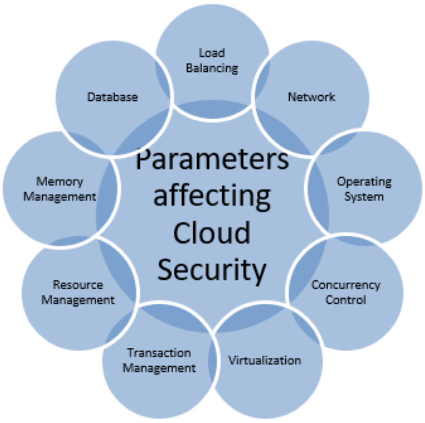

Figure 3: Factors affecting cloud security

Cloud storage services are suitable for the different security concerns of such services and technologies. For example, the network must be secured which interconnects the systems in a cloud computing. Furthermore, the cloud computing virtualization approach results in the numerous security issues. The mapping of the virtual structures to the physical systems, for example, must be performed safely. Data security involves encrypting the data and ensuring that the relevant techniques for data sharing are implemented.

Security Issues and Tips to avoid them

Digital transformation drive wide cloud computing adoption, allowing companies to access virtualized technology and accelerates innovation. Cost advantages provided by cloud infrastructures are obvious, but the security strategy can need to adapt to suit the differences in technology and operation.[6]

Few of the cloud security issues are:

1. **Gaining Visibility to identify cloud assets**: Large number of cloud apps has been used in every division of the organizations and it is very difficult for the security team to track which employee is accessing which data across the enterprise.

Companies transitioning from on-site infrastructure to the cloud will soon find themselves struggling to keep their cloud assets available, as each department is allowed more flexibility to deploy and use SaaS and IaaS solutions. The first step for security teams to take control is thus to obtain visibility.

Since the cloud assets lie outside conventional perimeters, a security framework designed specifically for this new environment is needed to provide insight into the cloud assets' inventory and security posture.[7]

Solution: Using protection solutions via API that include auto-discovery technology. Without shadow IT risk, you will be able to have an inventory of all your network, servers and job loads. They save you time and send you a detailed summary of all your deployments. Better still, incorporate a full stack protection tool that can provide an objective single glass panel view of the associated risks between on-site and cloud properties.

2. **Lack of staff with skill**s: In the aftermath of our latest survey, 17 percent of companies missed a critical security flaw because they did not have the expertise to rectify it, while 25 percent overlooked a critical security flaw because they had no time to repair it.

Two thirds (64 percent) of UK IT decision-makers, however, said their companies are losing revenue because they don't have the cloud expertise needed.

With more than one hundred separate services for each cloud provider (e.g. 142 AWS services), security teams are unable to keep up with and efficiently apply all the best security practices.

If businesses do not have the necessary cloud knowledge in-house, risks will quickly outweigh the benefits provided by the cloud.

Solution: It's extremely difficult to locate and recruit staff with deep cloud security experience; you have to worry of outsourced services from information security firms. MSSP or software companies with strong cloud competency may be an excellent choice to direct your company through configuration and help adjust security policies to your cloud environment before you create enough cloud experience in organization.

3. **Follow best practices in security for your cloud configuration and workloads**: A recent study by 175 security professionals reveals that, as soon as they are discovered, only 50 percent of organizations patch vulnerabilities, 15 percent wait for a month, while 9 percent agree to submit patches only once or twice a year. If you think the only one responsible for the security safety of your data in the cloud is Infrastructure as a Service Provider, think again.

Deploying cloud computing software and data doesn't protect you from bugs and application and data limitations. Remote workloads have their own weaknesses, and are risky assets because conventional security strategies do not incorporate Remote Workload Safety technologies. You need to track the infrastructure constantly, and apply corrections and patches to stay safe.

Solution: At the one side, a standardized architecture is deployed and configured that follows the AWS Foundations Benchmark Center for Internet Security (CIS) and the Microsoft Azure Foundation Benchmark CIS.

At the other hand, use an automated vulnerability management system to constantly monitor the environment for your protection at workloads.

4. **Beware of APIs**: In 2018 alone, we saw at least half a dozen high-profile data breaches and vulnerabilities to security caused by weak protection of APIs (Salesforce, Panera Bread, Vemno ...). And this doesn't even include cases involving T-Mobile, Instagram, and McDonald's that all together revealed personal data about millions of their users. Application programming interfaces (APIs) are all the rage as developers now depend heavily on them to support product and service delivery and integration. These are the front door open to your submission, and need to be publicly available by

nature. Cloud services allow access by third parties through the disclosure of APIs, but many DevOps and companies ignore the significance and fail to protect APIs.

Solution: Respect protection with design approach to production of applications. This approach would allow companies to understand the security requirements around publishing APIs and construct adequate authentication and ensure that the code itself does not contain any obvious vulnerabilities.

5. **Train the users to follow best practices in safety**: IaaS providers discuss their current cloud protection practices. Your users will consider the top 10 best security practices for AWS or the top 10 best safety practices for Microsoft Azure. The behavior of employees may be the most important front door to cyber-attack, without adequate training. IT leaders need to ensure that cloud customers know best practices as this is the only way to protect the company's infrastructure from misconfigurations.[8]

Solution: Organizations should also recognize and encourage ambassadors of awareness — cloud users dedicated to security measures and urging their colleagues to do the same — this will help improve the security posture of the entire enterprise.

2. CONCLUSION

The service provider and the client will be completely confident that their data in the cloud is fully secured from getting hacked from outside world, and that the customer provider will have a clear and shared understanding. The biggest gap between cloud security implementations and research theory lies in the fact that the research concept leaves some major gaps between real cloud protection and virtual machine protection. Work will focus on and eliminate these gaps and disparities.
Some of the approaches could be to build a method for tracking cloud computing software, and the other could be the development of independent processing for different client applications.

REFERENCES

1. Jahangeer Qadiree, Mohd Ilyas Maqbool, “Solutions of Cloud Computing Security Issues” - International Journal of Computer Science Trends and Technology (IJCS T) – Volume 4 Issue 2, Mar - Apr 2016.
2. Sabiyyah Sabir, “Security Issues in Cloud Computing and their Solutions: A Review”- International Journal of Advanced Computer Science and Applications,Vol. 9, No. 11, 2018.
3. Arun Kumar Sen, Pradeep Kumar Tiwari, “Security Issues and Solutions in Cloud Computing” - IOSR Journal of Computer Engineering”, Volume 19, Issue 2, Ver. IV (Mar.-Apr. 2017), PP 67-72.
4. Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull, “Security Issues with Possible Solutions in Cloud Computing-A Survey”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.
5. B. Anandkumar, Chaitrali S. Dangare, A. Manusha Reddy, Y. Indu and B. Padmaja "A survey on security in cloud computing" Journal of Advanced Research in Dynamical and Control Systems Special issue(11) 82-86 (2018)
6. G. Prabhakar Reddy, K. Sai Prasad, N. Chandra Shekar Reddy and R. Karthik, 2018. Privacy Preserving and Data Publishing using Tuple Grouping Algorithm. Journal of Engineering and Applied Sciences, 13: 930-933.
7. B. Madhuravani, Dr. P. Bhaskara Reddy, Dr. Sheikh Gouse, Swapna Bhumandala, “secure authentication and dynamic encryption using ecc and wireless networks”, Journal of Advanced Research in Dynamical and Control Systems, ISSN: 1943-023X Issue: 12-Special Issue, 2017, Pages: 1131-1144
8. B. Madhuravani, Dr. D.S.R. Murthy, ” A Hybrid Parallel Hash Model Based On Multi-Chaotic Maps For Mobile Data Security”, Journal of Theoretical and Applied Information Technology, Volume 94, No.2, ISSN: 1992-8645