CLOUD COMPUTING : SECURITY CHALLENGES AND ISSUES

Simar Preet Singh¹, Supriya Shrivastav², Neeraj Singla³, Harmandeep Kaur⁴
¹²³⁴Computer Science and Engineering Department, Chandigarh Engineering College (CEC), Landran, Mohali

ABSTRACT

Over the past few years, Cloud Computing has grown extensively. Many companies can no longer sustain without transitioning towards cloud computing platforms. Cloud can provide companies the fast access to their business applications and significantly augment their infrastructure resources. Since the demand for cloud is increasing tremendously, one needs to look at the aspect of cloud security. Security acts as a backbone of any technology. Security in Cloud helps in protecting data from theft, getting overwritten or deletion of the data, natural disasters or even prevents from data leakage. This technology uses the concepts of tokenization and other means like Virtual Private Networks (VPNs), hardware and software based firewalls etc. to enhance security. Cloud Security is such a topic that one can dig deeper to find the root causes for the potential threats. This forms the basis of this research paper wherein we are going to do research about the issue related to cloud security and the challenges that the organization may be facing or can face in the future.

Keywords: Cloud security, challenges, cloud computing, cloud service, security issues.

I. INTRODUCTION

For the past few years, cloud computing has become fastest growing segment of the technology industry. Cloud computing comprises of accessing online software applications, processing power, use of social media, some forms of interpersonal computing and data storage. According to US National Institute of Standards and Technology, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

In the current scenario, where the presence of cloud computing has increased a lot, a pivotal role is being played by the data-center which is controlled by big multinationals like Google, Microsoft Azure, Salesforce and Amazon that provides the cloud infrastructure. Some of the characteristics of cloud include: the ability of resilient computing, homogeneity, service orientation, massive scaling, low cost software's and virtualization [2, 3]. Some of the essential characteristics of cloud computing are:

- Broad network access: Standard mechanism promotes use of thick and thin client platforms which include laptops, workstations, tablets, mobile phones etc.
- Resource Pooling: A multi-tenant model is followed in which all the computing resources are pooled to serve multiple consumers having varied physical and virtual resources which are assigned and reassigned dynamically depending upon the demands of the consumer.
- On-demand self-service: Eliminating the requirement of human interaction with the service provider, a user can himself change the computing capabilities according to her/his use such as server time and network storage.

Cloud Computing has mainly three service models, which includes:

- Software as a Service (SaaS): SaaS has a cloud infrastructure on which applications run. These applications can be used by the cloud users on subscription basis. Either thick clients such as computers and laptops can be used or thin client interface such as web browsers and web
based emails or program interface can be used to gain access to the applications running on the cloud. The base cloud infrastructure, which includes operating systems, storage, network or servers, are not controlled by the users of the cloud computing platform. With the feature of limited user specific application configuration setting, some of these can be controlled by the user [2].

- Infrastructure as a Service (IaaS): IaaS provides virtualized computing resources such as processing, storage, networks over the internet. Users can deploy and run softwares. Amazon Web Services and Flexi-Scale are examples of infrastructure as a service [3].

- Platform as a Service (PaaS): Users have the choice to engage cloud infrastructure for consumer created and acquired applications which can be made using the infrastructure provided by the service provider, libraries, programming languages, services etc. [4].

Cloud Security is one of the parameter which is still stopping corporates and small industries to transition towards the cloud computing. Security threats are only increasing with the passing days. These threats are becoming more sophisticated with the rapid invention of technology. It is imperative to build a robust cloud platform without any risk of security. This paper talks about the existing threats to cloud security and how we can try to improve the current scenario and help industry bloom to its fullest potential.

II. RELATED WORK

A research was conducted by Cloud Security Alliance (Cloud Computing Alliance) in 2010 which narrowed down the major threats to cloud security to the following points [5]:

- Provider Security Failure
- Availability and Reliability Issues
- Perimeter Security Model Broken
- Shared Technology Vulnerabilities
- Data loss/leakage
- Attacks by other users
• Legal & Regulatory Issues
• Abuse & evil use of Cloud Computing
• Insecure API

Security measures are set up and researchers started working on all these threats. Later, another survey was conducted by International Data Corporation (IDC) of about 250 IT executives to gain insight of their views and that of the companies for which they are working about the cloud services [6]. Figure 1 shows the results of this survey. The biggest backdrop of the cloud computing was the issue of security. Figure 1 shows that security is considered as the biggest challenge on the cloud model with about 87.5% people thinking not to transition to cloud because of this security concerns.

The objective of this paper is to find out various issues pertaining to the cloud computing platform. This paper also includes the types of challenges faced by the industry. What are the major drawbacks related to cloud security as well as what type of threats are majorly occurring in the current cloud system along with what steps can be taken to avoid these threats so that easy transmission can take place without any hindrance.

III. ISSUES IN CLOUD COMPUTING

Security is one of the major issues faced in cloud computing. This is all because the system that is used to provide the cloud service does not belong to us (i.e. user). The user basically knows nothing about what could happen to their data. This issue becomes more dangerous when the data that was stored on the cloud system is personal or contains valuable information of the user. Privacy of users cannot be compromised so the cloud service provider companies need to ensure that the user data is safe and secure. This has become increasingly challenging due to the advancement of the technologies because whenever the security development is done there is always someone who can breach the security and take advantage of the data present [7, 8].

Following are the types of issues which are usually encountered when discussing Cloud Security:

• Data Issues: As being one of the advantages of cloud computing that users can access their data anywhere they want and anytime they want. This means that there are many consumer/service providers of cloud computing who can access the data and can modify the data also. Many cloud service providers rather than providing their own servers, they acquire servers from other service providers due to its cost-effectiveness and flexibility for operation. So the probability of user data getting stolen increases a lot as it can be stolen from the external server. Moreover, if the company does not have any backup storage of the user's data, then if there is a natural disaster than the entire user's data will be lost. If the company closes down due to financial or legal issues then the entire user data will be lost again [9].

• Privacy Issues: Privacy issues are also one of the major issues. The user's data that was stored upon the clouds can be their personal/valuable information and this information is far more important to be protected from other users and other service providers as most of the cloud computing companies acquire servers rather than providing their own servers. To protect user's privacy, the companies must keep the track of who is accessing that information and who is maintaining that server [10].

• Infected Application: Infected applications can be harmful as they can keep the track of our data and sometimes even control our machines etc. So cloud service provider must not let any user to upload any infected application which could severely affect the system [11].

• Flexibility Issues: Cloud service provider companies need to be flexible with each other as due to some reasons if a user has to move from one cloud service provider to the other and if the companies are inflexible with each other then it will be really difficult for the user to start from scratch for the other service provider [12].
Virtual Machine Security: Virtualization is considered as one of the main components of cloud computing. Virtual machines are not static; they are dynamic, which means data can be lost i.e. it can be reverted back to the previous instance; it can be paused and restarted easily. In virtualization, different instances that are running on the same physical machine are isolated from each other. This dynamic nature and potential of the virtual machine makes it difficult to maintain consistent security. In cloud computing, there are two types of virtualization: full virtualization and paravirtualization. In full virtualization, entire hardware architecture is replicated virtually but in paravirtualization, only the operating system is changed so that it can run concurrently with other operating systems. VMware's shared folders mechanism that grants users of a guest system to read, write and access any portion of the host's file system including the system folder and other security-sensitive files, is one of the major vulnerabilities that virtual machines have [13].

IV. CHALLENGES IN CLOUD COMPUTING

Research on cloud computing is still on the early stage and many of the issues have not been resolved perfectly but still due to increasing development in technology, new challenges always come up in the way of cloud computing. Following are some of the challenges that cloud computing has to face:

- Data Encryption: Encryption is widely used to maintain secure access to the data. Security can range from very simple security (not so secure) to highly secure. You and the provider of the cloud computing solution, have many decisions and options to consider like the web app that we want to use. It provides SSL encryption for access and when the object arrives at the cloud it is decrypted and stored so as it necessary to encrypt it before storing etc. [14].

- Access Controls: Authentication and identity management is more important than ever. What level of enforcement about password strength and change frequency does the service provider invoke? What is the recovery methodology for the password and account name? etc. This is not all that different from how you secure our internal systems and data, and it works the same way, if we use strong passwords, that changed frequently with typical IT security processes, we will protect that element of access [11].

- Platform Management: Cloud platforms provide different kinds of platforms to write applications that use services provided from the cloud or that run in the cloud or both. These platforms are on-demand platform and platform as a service challenges in delivering middleware capabilities for building, deploying, integrating and managing applications in a multi-tenant, elastic and scalable environments.

V. RESULTS AND DISCUSSIONS

Cloud Computing is early at research so rather than being a great technology it has to tackle many issues and challenges along the way. The issues and challenges discussed above are not only issues and challenges that cloud computing has faced as there are many more issues and challenges that cloud computing has to face in future also.

5.1. Solutions:

Some of the proposed solutions to overcome Cloud Security Issues are as follows:

- Selection of Cloud Service Provider: Select the cloud service provider correctly as we can find various cloud service providers out of which many will not have their own servers and providing service by acquiring the servers. Also, cloud vendors must have experience and be well established to be far away from closing down in the near future. If still for some reason cloud vendors need to shutdown then the user must have clear contact with them and a user must get
notified before they are going to close down. In such situations, the user can transfer their data to other cloud service provider. For selection, the cloud service provider user should check that cloud service providers must be flexible with the other cloud service provider as well, so in case if they need to shut down user can transfer their data to other cloud service providers [15].

- Recovery Facilities: Every cloud vendor must have a great recovery facility. So that if data gets lost or gets corrupted, the user can recover the data easily. For that, cloud vendors must have great backup storage facilities [11].

- Encryption: Encryption is far more the most important solution needed. The encryption provided by the cloud service provider for user data, must be well secured so as the user’s personal/valuable data cannot be accessed by anyone. Only the authorized user can have access their personal/valuable data. The user data must be encrypted even before storing it to cloud storage so that even if someone hacks the cloud system, he/she has to further decrypt user data to understand.

VI. CONCLUSION AND FUTURE DIRECTIONS

Cloud Computing is a great technology that will be used for personal usage and not only for storing data but for streaming the movies, games, etc. in the near future. Cloud computing is still in the early research area with many of its issues and challenges still remain unresolved. Cloud Security, one of the major issues cloud computing is facing nowadays. With every development in security, there is always someone who will be able to breach the security and access user’s data. There are many aspects of security issues like network and virtualization issues albeit this paper only discussed some of the issues of cloud security. Security techniques need to be tweaked on a regular basis so that security will be maintained. In future, cloud security must be enhanced with latest encrypted techniques and algorithms to provide enhanced data security to the user.

REFERENCES


