An Analysis on Security Threats in Cloud Computing

Dr. A. P. Nirmala [#1], R.Prema [*2], Dr. B. Meenakshi Sundaram [#3]
[#1*2#3] *MCA Department, New Horizon College of Engineering*
[1] nirmalasuresh.ap@gmail.com
[2] premabit@gamil.com
[3] bmsundaram@gmail.com

***Abstract*— Cloud Computing is a paradigm that changed the way of storing and accessing data and computing power. Today the business companies don't have to depend on physical infrastructure for storing tones of data rather they store their data on virtual platforms which helps them to work on how to grow their business more. Cloud Computing is the delivery of computing services such as virtual servers, virtual storage, networking, software, analytics and much more via the internet. This paper presents an overview of cloud computing which is the prominent technology nowadays. It provides an analysis on cloud computing security and the threats imposed on cloud computing. It also highlights few measures to prevent the attack from the business perspective.**

***Keywords*— Cloud security, Malicious insiders, DDoS, Data Breach. Account hijacking, Security Threats**

I. INTRODUCTION

"Cloud Computing is the on-demand delivery of compute power, database storage, applications and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing"[8]. In simple definition cloud computing is a virtual environment of delivering computing services such as servers, storage space databases, networking, analytics and much more over the internet. As an example, let's say you are the owner of a business and large amount of data is being generated every day. You don't have enough space to store those data. Your One Drive, Google Drive spaces are limited. Servers can't hold that much amount of data or else it will slow down. So, what should you do now? In these types of situations cloud services plays its important role.

Cloud computing provides large size storage where you can store your large amount of data generated every day. Not only you can store and recover, you can also use this technology for hosting servers and virtual machines, can deliver software applications over the internet and also use on-demand environment for developing, testing, delivering and managing software applications. 'Cloud Providers' which refers to the data centres or individuals who offer other customers computing services by charging them on usage basis similar to the bill of post-paid internet service that you use from particular telecom company.

Cloud security is protecting your confidential data which the business owner, stores on online virtual storage such as Amazon web services (AWS), Google cloud platform. various set of rules, policies and data protection technologies have been put forward by cloud providers in order to prevent and avoid any unauthorized access and exploits of customer's and business organization's data.

This paper is organized as follows. Section II emphasizes the benefits of cloud computing and section III provides the security issues addressed in few related works. Security challenges are analysed in section IV followed by the conclusion in section V.

II. BENEFITS OF CLOUD COMPUTING

A. Cost

Cloud computing rules out major capital expenses of buying hardware and software, setting up and running of on-site data-center eliminates the cost of servers, cost of IT experts for managing the infrastructure.

B. Speed

In cloud virtual environment, it takes only minutes to make resources, of any type, available for developers so that they don't have to delay their project's deployment. This results in dramatic increment in agility for the organization.

C. Global Scale

The biggest benefit of cloud computing is providing scalability on global scale. That is delivering right amount of IT resources when it is needed and from the right geographical location.

D. Productivity

According to Microsoft, on-site data-center normally requires a lot of racking and stacking. It simply means that you have to set up hardwares for your data-center, then requires software patching and various time-consuming works. Cloud computing removes all these troubles so that IT teams can spend time on achieving their goals.

E. Performance

The cloud computing services run on a worldwide network of data-centers which are regularly updated to latest generation of fast and efficient computing hardware making these data-centers safe and secure.

F. Reliability

Cloud computing provides data backup, recovery option from any disaster since data are mirrored/copied to multiple sites on the cloud virtual network [2].

III. Related Work

In this section, key issues and possible solutions by various researchers on cloud computing security are discussed.

Ms. Disha H. Parekh and Dr. R. Sridaran [1] have addressed various security challenges in cloud computing such as data leakage problems, malicious attacks, service hijacking, virtual machine hopping etc. They have also presented various security challenges which are, cloning and resource pooling, authentication and identity management, unencrypted data etc. They also have deduced that security challenges are imposed in case of network too. Such challenges are SQL Injection attack, flooding attack, browser security etc. They have analysed that there are various security threats in regards to deployment and service models. According to them, since cloud services are provided over internet the users/customer needs to thoroughly examine all kinds of network security threats. They suggested that in order to utilize the power of this robust technology the cloud providers need to take and implement positive and practical counter measures in order to guarantee security of data.

According to Jeff Beckham [7], cloud computing although provides considerable cost-saving benefits such as pay-as-you-go but when using cloud-based services one should keep in mind top five security concerns such as secure data transfer, secure software interfaces, secure stored data, user access control, data separation.

Mr. Pradeep Kumar Tiwari and Dr. Bharat Mishra [3] have discussed about cloud computing architecture and also addressed various types of threats in cloud computing like failures in provider security, availability and reliability issues, malicious insiders, shared technology vulnerabilities etc. They have provided few solutions to deal with various types of cloud computing security which are:

Clear contract: a clear contract should be established with cloud vendor so that in case cloud vendor closes before the agreement, the enterprise or customer can claim.

Find key cloud provider: the first solution they have suggested is to find right cloud service provider. Different vendors will have different cloud IT security and data management. So, it is necessary to choose a cloud vendor who is well established, have experience and implements industry standard and regulations.

Better enterprise infrastructure: enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers as well as software such as operating system. Enterprise should have measures implemented in order to prevent cyber attack.

Recovery facilities: the cloud providers should implement excellent data recovery mechanisms. This will help the cloud providers to easily manage the continuity of data by recovering crucial and confidential data which are either lost or fragmented due to certain issues.

Mohsin Nazir in [4] has discussed about various types of challenges in cloud computing. Among those various types, the most noticeable ones are:

Data Encryption – encryption is the key technology in case of data security. Whether the data is at rest or whether data is in transition, encryption plays an important role in both the cases. The author in [4] told that the user/customer has to understand that whether the cloud service providers, that uses APIs to provide access to cloud, provide SSL encryption which is considered to be standard or not? The author also mentioned that the user/customer has to ask them self that whether they want to encrypt the file before uploading to cloud or do they prefer that cloud service provider encrypt their files automatically.

Service Level Agreements (SLA) – the biggest challenge for cloud customers is evaluating SLAs of cloud vendors since cloud service is governed by Service Level Agreements [5] that allow several instances of one application is copied to multiple servers. According to Mr. Nazir, cloud vendors prepare SLAs in order to set a defensive shield to protect them from legal actions while their assurance of security and protection is not up to the mark. The customers before signing contract with any cloud vendor must first take into account the data protection, encryption techniques, price structures, etc. provided by vendors.

Access Controls – authentication and identity management is more important than anything else for securing your data. It implies that what level of application of strong password and change frequency does the cloud service provider put forward? Is there any password recovery and account name recovery methods present? Do they notify customers about password change of their account? These methods are no different than the methods that are applicable to normal internet-based services such as Email.

IV. ANALYSIS ON SECURITY THREATS IN CLOUD COMPUTING

In today's world, every business is moving towards cloud virtual storage since the expense in cloud virtual storage is very less compared to investing on physical hardware and IT managers to maintain the physical hardware. But there are certain challenges that every cloud providers today faces. Such security challenges are:

A. Distributed Denial of Service Attack (DDoS)

Distributed Denial of Service has been targeting various service providers from long time. During the first quarter of 2015, Verisign reported that DDoS attacks targets most frequently the IT services, Cloud and SaaS. It has been designed to overpower the website servers so that they no longer can respond to the requests of legitimate users/customers. If DDoS attack is successful, then it renders website useless for hours, even for few days.

B. Securing Sensitive Data

62% companies store their sensitive customer data in the public cloud and 40% organizations delegate cloud services without concerning the IT departments. This makes organization prone to data breach and also, they have to face lawsuits, fines and damaged public reputation if and when data is breached.

C. Insecure Access Points

The greatest advantage of cloud virtual storage is that it can be accessed from any place at any time from any device. But the question that arises is what if the interfaces and APIs that cloud services uses; with the help of which customers interact aren't secured? For hackers this kind of vulnerability is like finding a golden egg laying chicken.

D. Account Hijacking

For cloud services account hijacking or service hijacking adds another threat to their environment. If any hacker gains access to a user credentials then they have full control over activities and transactions of the user, they can manipulate data or can return inappropriate information or even can redirect to illegitimate sites. With stolen credentials, cyber attackers often access critical areas of cloud computing services resulting in compromise in confidentiality, integrity and availability of those services.

E. Malicious Insiders

This is the biggest for cloud providers because malicious insider could be anyone such as System Administrator. System Administrator can access sensitive information which he can exploit by all sorts of ways. If the system administrator has access to sensitive information then he/she have access to more critical system of increasing levels and eventually to data [6].

F. Data Breach

Data security is of utmost importance for any business organization and it has the top priority than anything else. Breaching confidential data stored in the cloud is the most dreadful threat for cloud providers and major concern for IT leaders. Breaching of confidential data includes information such as trade secrets, intellectual property information, personal health care information, financial reports, personally identifiable information etc.

However, a few steps which help any business organization to prevent their confidential data from being prone to any kind of attack are:

1) Clear contract should be established between cloud vendor and customer. This helps the customer to claim refund in case the cloud vendor shut down their operation.
2) High level data encryption should be implemented by very cloud service provider during its transit as well as when it is at rest.
3) An adaptive model – based approach in tackling the cloud security problem should be implemented by every cloud vendor. This model will help in problem abstraction and understanding the security requirements of different stakeholders at different level of details.
4) Transparency should be implemented between the cloud service provider and customer so that the customer has detailed information on cloud provider's security architecture.
5) Use of firewalls and user access control are strong measures in order to prevent any kind of attack on confidential data.

V. CONCLUSION

Since every technology will always have vulnerabilities and we also know that there can't be a 100% robust, safe and secure application but what can we do is we can provide or develop some counter measures to stop or prevent any kind of attacks on cloud virtual storage. This paper provided an analysis on security threats in cloud computing and research on providing possible solutions for various types of threats on cloud computing which is need of the hour. Thus provides the future directions for the researcher to develop robust technique which can be implemented to cloud virtual storage technology in order to make this technology safe and secure with good gains to cloud customers.

REFERENCES

[1] Ms. Disha H. Parekh, Dr. R. Sridaran, "An Analysis od Security Challenges in Cloud Computing", *IJACSA*, Volume: 4, Number: 1, 2013.

[2] Rabi Prasad, Padhy, Dr. Manas Ranjan Patra, Dr. Suresh Chandra, Satapathy, "Cloud Computing: Security Issues and Research Challenges", *IJCSITS*, Volume: 1, Number: 2, December 2011.

[3] Pradeep Kumar Tiwari, Dr. Bharat Mishra, "Cloud Computing Security Issues, Challenges and Solution" in *IJETAE*, ISSN: 2250-2459, Volume: 2, Issue: 8, August 2012.

[4] Mohsin Nazir, "Cloud Computing: Overview and Current Research Challenges", *IOSR-JCE*, ISSN: 2278-0661, Volume: 8, Issue: 1 (Nov. – Dec. 2012).

[5] Irfan Hussain and Imran Ashraf, "Security Issues in Cloud Computing – A Review" in *International Journal of Advanced Networking and Applications*, Volume: 6 Issue: 2, ISSN: 0975-0290.

[6] Sabah Naseem, Prof. Ashish B. Sasankar, "Cloud Computing Challenges and Related Security Issues" in *IOSR-JCE*.

[7] Jeff Beckham (2011), "Security Risks of Cloud Computing", in Cisco Blogs by Cisco [ONLINE] available in https://blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud-computing

[8] Dr. A. P Nirmala and Dr. R. Sridaran, "Cloud Computing Issues at Design and Implementation Levels – A Survey", IJANA,Volume: 03, Issue: 06 ISSN: 0975-0290 (2012).