Volume 8, No. 2, March 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Security Challenges and Threats in Cloud Computing Systems

Hiba Khan
University Women's Polytechnic
Aligarh Muslim University
Aligarh, India
hibakhan091@gmail.com

Mohd Vasim Ahamad
University Women's Polytechnic
Aligarh Muslim University
Aligarh, India
vasim.zhcet@gmail.com

Abdus Samad
University Women's Polytechnic
Aligarh Muslim University
Aligarh, India
abdussamadamu@gmail.com

Abstract: During past few years, the internet has accelerated the use of computing devices like computers and mobile Phones. These devices are generating huge amount of data for the users on daily basis. Cloud computing provides computing, storage, services and applications over the Internet. It is one of today's most popular technologies due to its low cost computing with increased flexibility, scalability mobility and enhanced storage. Data generated by users over internet are stored on some remote location with respect to the user. This is the reason why IT organizations have shown their interests over security of cloud computing implementation. The main objective of this paper is to provide the critical review of the different vulnerable security issues of the cloud computing systems.

Keywords: Cloud Computing, Security Threats, Information Security, Challenges of Cloud Computing

I. INTRODUCTION

Nowadays, IT organizations considers the cloud computing as the most popular internet based services. Cloud computing enable users to communicate information, services or applications from remote location without having a costly and complex hardware and/or software infrastructure. The basic aim of cloud computing is to provide access to the information, services and the application from anywhere at any time without the need for hardware equipment [2]. Data and services need not to be stored to a storage device on one's PC. It minimizes the overall cost of accessing the information and services.

Using cloud computing, users can access data, generated by herself and others, stored on remote servers using internet (e.g. Google Drive, Dropbox, iCloud). It is considered as the major evolution in current internet technologies because of the flexibility, scalability, and management provided by cloud computing platforms and services. As information and services are shared on internet, there is a strong need to understand the different issues associated with it. By analyzing these security issues, it is possible to find solutions to prevent them.

This paper is organized in five sections. Section I is Introduction. Section II describes the concept of cloud computing and its applications. Section III gives a detailed review of various security challenges in Cloud Computing system and section IV deals with different types of threats. Section V concludes the paper.

II. CLOUD COMPUTING CONCEPTS

Cloud computing enable users to communicate information, services or applications from remote location without having a costly and complex hardware and/or software infrastructure. Cloud computing systems would reduce the need for advanced hardware on the user's end.

Users need not to buy the state of the art computers with the huge storage capacity, all of this is done by the cloud computing system. The only thing needed to access cloud services is a terminal consists of a monitor, an input device such as keyboard and mouse.

The terminal should have enough processing power to run the cloud computing application at user's end. As a user, you wouldn't need a huge storage capacity because you'd store information on some remote computer.

The customers of cloud computing do not need to have storage capabilities or the physical infrastructure to access the information. The cloud computing services can be categorized into three important service models. These models clearly defines how cloud computing services are being provided to users.

1) Platform as a Service (PaaS): This service model provides the capabilities to build services and applications from the scratch. It provides a platform which includes application/services design, it development, hosting, database integration, web services development & integration, security options etc.

2) Software as a Service (SaaS): This service model provides access to various software applications and resources stored on some other remote location using internet.

3) Infrastructure as Service (IaaS): It enables users to access infrastructure resources like network resources, hardware resources, data storage, etc as a service.

Characteristics of Cloud Computing

The Cloud computing can be defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computer resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[7]. There are following most important characteristics of cloud computing amongst many.

1) *On-demand Services:* A user can access computing resources, such as information, services, application, network infrastructure, and data storage without any interaction with each service provider.

SEMINAR PAPER
National Seminar on Cloud Computing and its Applications (March 9-10, 2017)
Organized by
Dept of Comp. Sci. & Eng, SEST, Jamia Hamdard, New Delhi (India)

2) *Universal Access:* A user can access computing resources using their phones, PDAs, laptops, and PCs. They can use these devices irrespective to location of the user.

3) *Resource Pooling:* The cloud computing resources (data storage, applications, processing, and network bandwidth) are pooled at some servers to serve its users as and when they need.

4) *Scalable & Elastic Services:* the cloud computing services are made flexible and scalable to suit the user's immediate needs. The software resources, users and other features can easily be added or deleted without making any inconsistency.

5) *Measured Services & Management:* Cloud computing provides many benefits for user and cloud service providers by minimizing cost and maximizing flexibility. Cloud computing resources used by users can be monitored, controlled and reported, providing transparency for the service providers and users.

Applications of Cloud Computing

Cloud Computing is one of today's most popular technologies due to its low cost computing with increased flexibility, scalability mobility and enhanced storage. Data generated by users over internet are stored on some remote location with respect to the user. These factors have made cloud computing an active component in the following application areas.

1) *E-Learning:* E-learning is the most popular evolution in the field of education. It provides an attractive solution for learning over internet without having own network infrastructure and storage capabilities. Students, faculties, researcher scholars can connect to the cloud via internet and access information and services.

2) *Enterprise resource planning (ERP):* Enterprise resource planning (ERP) is a business process management software that allows an organization to use a system of integrated applications to manage the business, applications, services, human resources, payrolls etc. It is very expensive for organizations to have their own ERP infrastructure. To deal with it, cloud service providers install ERP system in the cloud itself which can be used by multiple organizations.

3) *E-Governance:* By expanding the availability and scalability of services, service providers can improve the functioning of a government by improving the way it provides the services to its citizens and. It also minimizes the overhead of managing, installing and upgrading applications and services.

Some important features of Cloud Computing

Cloud computing enable users to share information and services from remote computer without having a costly and complex hardware and/or software infrastructure. There are following important features of cloud computing:

- Cloud computing uses *'Pay as you use'* business model.
- It Shares resources and information to number of users simultaneously.
- One of the essential component of cloud computing is virtualization. Virtualization is one of the hardware reducing, cost saving and energy saving technology.
- User can access applications as utilities and information, over the Internet.
- User as well as service providers can manage the application and data at any time using the Internet.
- In cloud computing user need not to install a specific piece of software to access information and services over cloud.
- Cloud computing provides online tools for development and hosting, runtime environment for programming.
- Cloud computing provides platform independent access to resources and information over the Internet all users.
- It offers on-demand self-service. The resources can be utilized without interacting to the service provider.
- Cloud Computing is highly cost effective because data and services need not to be stored to a storage device on one's PC. It minimizes the overall cost of accessing the information and services.
- Cloud Computing offers load balancing to distribute the excessive load on a particular server. This feature makes it more reliable.

III. SECURITY CHALLENGES IN CLOUD COMPUTING

Although cloud computing systems are capable enough for organizations to share information and services using internet without any need of physical infrastructure, it is vulnerable for security threats which must be solved. As information and services are shared on internet, there is a strong need to understand the different issues associated with it. There are following security challenges of cloud computing.

Confidentiality

Confidentiality can be defined as the ability for an authorized group of users or authorized systems to access protected data [4]. The increase in number of users of cloud computing systems helps in increasing the access points; hence the data becomes more exposed to external entities and more likely to be compromised [4].

1) *Data Confidentiality:* Data confidentiality is all about to provide access control to the data, memory and devices. It is the property that data contents are not made available or disclosed to illegal users. Therefore, we need to provide a strong secure verification system which may leads to secured access within Cloud services [4].

2) *Application Confidentiality:* Cloud services also provide access for software applications eliminating the needs of installing them at every system. Hence, application security can be another important factor for providing a secure cloud system [4].

Privacy

Privacy is the ability of individual user/system or group of users/systems to control the sharing of data to other users or systems. Individuals are required to follow rules set by governments concerning user's personal data privacy and

SEMINAR PAPER
National Seminar on Cloud Computing and its Applications (March 9-10, 2017)
Organized by
Dept of Comp. Sci. & Eng, SEST, Jamia Hamdard, New Delhi (India)

confidentiality. Because, data is stored on multiple locations in cloud network, they are vulnerable to security breaches [4].

Integrity

Data integrity can be defined as the means to protect data, services and application from unauthorized modification and deletion in cloud computing systems. Data integrity can be divided into following two categories:

1) *Data Integrity:* Data integrity is protecting data from unauthorized deletion and modification. The cloud service provider should ensure the users that personal data are not manipulated in between. Data integrity is very important factor in order to achieve a high level of confidentiality in data and system integrity. As number of users increase, number of access points to access cloud services increases, which, in turn, requires authorized access [4].

2) *Software Integrity:* Software integrity is basically restricting the unauthorized access and modification in software applications provided by cloud systems. The software application owner or administrator is responsible for software integrity from unauthorized modification [4].

Availability

Availability refers to the ability of an authorized user to access a cloud system and use it to share information, use cloud resources and application even with a security interruption or a system malfunction [4]. Availability includes the availability of data, applications and physical components on request of end user [4].

IV. Cloud Computing Security Threats

The issue of security relating to cloud computing is becoming more significant with the increased deployment. At the same time, cyber-attacks are also increasing with the increased use of applications [3]. Cloud service providers are making an extensive effort to secure the services and systems so as to decrease the threat of attacks and gain the confidence of their customers [4].

The main function of any cloud provider is to provide a cloud service which can secure resources or information on the cloud. In general the main issues of the cloud are related to the confidentiality & integrity of the data. There are some security threats that are limiting the boundaries of cloud services.

Broadly, security threats in cloud computing can be divided in the following categories:

- Web based Threats
- Application based Threats
- Physical Threats
- Network based security Threats

Web Based Threats

1) *Phishing scams:* It sends the links of those websites that are designed to get the personal data like account numbers, passwords etc. to the user via email, text messages, or any social networking site using a trick.

2) *Drive by downloads:* In this system the applications or some software gets downloaded without the authorization or user's knowledge which contains malware, spyware or viruses.

3) *Browser exploits:* Designed to want advantage of susceptibilities throughout a browser which is launched directly from browser or from third party extensions like Flash player, PDF reader, image viewer, etc. This can be made possible simply by visiting certain unsafe sites which automatically installs malware.[5]

Application Based Threats

1) *Malware:* It is the ability to rapidly connect and exchange content with anyone, anywhere which increases the chances of a cloud data breach.

2) *Spyware:* It assembles and use the personal and private information like location, contact list, email & photos without proper permission and utilize this information in future for cash fraud etc.

3) *Vulnerable Applications:* These are applications that contain faults & errors which can perform malicious functions. It may access confidential data, perform unwanted actions, stop a service from functioning properly, or transfer unwanted apps to your device.

Physical Threats

1) *Device Possession:* It is the ability to rapidly connect and exchange content with anyone, anywhere which increases the chances of a cloud data breach.

2) *Lost or taken devices:* In case the device gets lost or given to someone then it is of big concern for the owner as all the vital information nowadays are kept in mobile Phones.

Network Based security threats

1) *Network exploits:* It create the foremost of flaws as they will install malware on your device without your knowledge.

2) *Wi-Fi Sniffing:* It intercepts the information across the network when it travels and is unencrypted by scanning or any other means.

3) *Address Impersonation:* It means that no authentication is provided for the source and destination network addresses which can cause information to be delivered to some other unwanted addresses.[6]

V. Conclusion

In recent years, cloud computing has gained much response and spread round the globe. It is giving and extending its applications in almost every field be it business, shopping, education etc. However, the risk of the threats is the biggest problem users are facing today.

This paper elaborates the different types of applications of cloud computing and the possible threats associated with them. The analysis shows that all the threats can be put under four categories namely web based, application based, physical and network based. Therefore, in order to make a secure cloud computer system it is must to create a security framework which covers the different types of threats discussed here.

VI. References

[1] D.Huang, "Mobile cloud computing", IEEE COMSOC Multimedia Commun. Tech. Comm. (MMTC) E-Lett.6 (10) (2011)27–31.

[2] M.R. Rahimi, et al., "Mobile cloud computing: A survey, state of art and future directions", Mob. Netw. Appl.19 (2) (2014)133–143.01/04/.

[3] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz Hankel type involving products of Bessel functions", Phil. Trans. Roy. Soc. London, vol. A247, pp.529-551, April 1955.

[4] Zissis, D. and Lekkas, D. (2012) Addressing Cloud computing security issues. Future Generation Computer Systems. 28 (3), pp. 583-592.

[5] What is a mobile threat?, https:llwww.lookout.comlresources/know-your-mobile/what-isa-mobile-threat, visited on Mar 2017

[6] Solanke Vikas S., Kulkarni Gurudatt A., Katgaonkar Pawan, Gupta Shyam, "Mobile Cloud Computing: Security Threats" (2014)

[7] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing" in Special Publication 800-145 (Sept, 2011)