Various Challenges and Security Threats in Cloud Computing

Anu Kaul
Department of Computer Science
Sri Guru Gobind Singh College,
Chandigarh, India.
e-mail: kaul7anu@gmail.com

Khushwant Kaur
Department of Computer Science
Sri Guru Gobind Singh College,
Chandigarh, India.
e-mail: kkhushwantkaur@yahoo.com

Meena Gupta
Department of Computer Science
Sri Guru Gobind Singh College,
Chandigarh, India.
e-mail: meena.gupta355@gmail.com

Abstract— Cloud computing is an assimilation and on demand delivery of various information technology resources and services. The process is built to initiate real-time actions and responses for the enormous multi-dimensional data generated by websites, devices, applications and other sources. The cloud computing provides cost saving, flexibility, mobility to the clients along with disaster recovery and loss prevention providing sustainability and competitive edge without letting them to shell out for the requisite infrastructure, installation and manpower to achieve and maintain such hi-tech infrastructure. Maximizing the quality and quantity of service and resources besides limiting the infrastructural cost are important necessities for this technology. Cloud computing has transformed the way many organizations use and share data and applications over Internet by efficient distribution and utilization of their resources and services. With so much data going into the cloud, particularly into public cloud services, these resources have become susceptible to various security threats and challenges. In this paper we have discussed some of the critical security concerns that prevent the adoptability of cloud computing.

Keywords- *Cloud Computing, Cloud Delivery Models, IaaS, PaaS, SaaS.*

*****

I. Introduction

The demand for any organization today is improvisation of their resources with the minimal increase in the infrastructural cost. Cloud computing helps the industries to achieve great performance form their computer hardware and software resources at low cost. Cloud computing is based on utility and consumption of computer resources efficiently. Cloud computing technology involves deployment of groups of remote servers and software networks that allow data from different sources to be uploaded for real time processing to generate computing results.

The fundamental idea of cloud computing was pronounced way back in 1960 by Professor John McCarthy, as; “If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry”. Douglas Parkhill gave the characteristics of cloud computing in 1966 in his book “The Challenge of the Computer Utility”. Cloud computing had been a buzz word for many years and later turned into reality in 2007 when IT giants Google and IBM announced a collaboration for this concept followed by “Blue Cloud” announcement by IBM [1,2,3].

II. Cloud Computing

The National Institute of Standards and Technology (NIST) Information Technology Laboratory, cloud computing is defined as follows: “*Cloud computing is a model for enabling 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*” [4].

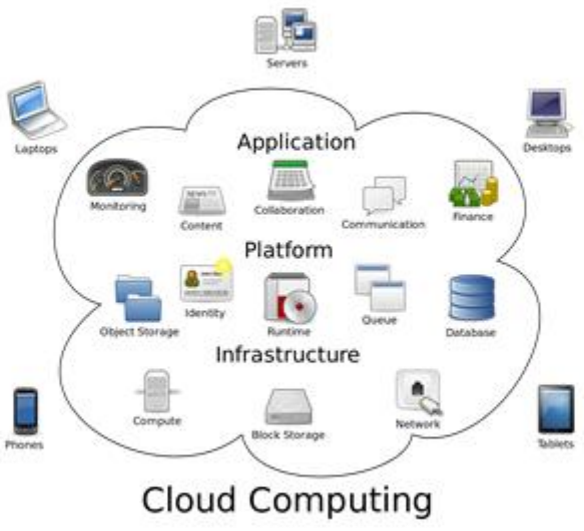

Fig1: Cloud Computing (Image Source: en.wikipedia.org)

There are four basic cloud delivery models, as outlined by NIST. The agencies may employ one model or a combination of different models for efficient and optimized delivery of applications and business services. These four delivery models are [4]:

(i) Private cloud in which cloud services are provided solely for an organization and are managed by the organization or a third party. These services may exist off-site.

(ii) Public cloud in which cloud services are available to the public and owned by an organization selling the cloud services, for example, Amazon cloud service.

(iii) Community cloud in which cloud services are shared by several organizations for supporting a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). These services may be managed by the organizations or a third party that exist offsite.

(iv) Hybrid cloud which is a composition of different cloud computing infrastructure (public, private or community). An example for hybrid cloud is the data stored in private cloud of a travel agency that is manipulated by a program running in the public cloud.

From the perspective of service delivery, NIST has identified three basic types of cloud service offerings. These models are [4]:

(i) Software as a service (SaaS) which offers renting application functionality from a service provider rather than buying, installing and running software by the user.

(ii) Platform as a service (PaaS) which provides a platform in the cloud, upon which applications can be developed and executed.

(iii) Infrastructure as a service (IaaS) in which the vendors offer computing power and storage space on demand.

Cloud computing is build on distributed computing, SOA networking, etc. these have numerous challenges associated with implementation and use of cloud computing. These challenges are required to be taken into consideration and optimal solution steps are to be taken up to overcome the problems so that quality of service can be improved and more users can be incorporated. According to survey of International Data Corporation (IDC), security, performance and availability are three biggest considerations in deployment of cloud. Other concerns are also present like resource management, identity management, performance, scalability, power and energy management.

III. VARIOUS CHALLENGES IN CLOUD COMPUTING

A. *Security and Privacy*

Stored and moving data, variety of resources and different security policies make security and privacy a critical challenge. Since, the data movement data storage and processing is not controlled by the organization which leads to high risks and vulnerable to malicious attacks. The security threats can be of two types: i.e. internal and external. The internal security risk is posed by organizational affiliates, current or former employees, contractors and other parties that have access to the cloud. External risks are posed by person and organizations that does not have direct access to the cloud like enemies and hackers. Cloud computing poses privacy concerns because the service providers may access, change or delete the data that is on the cloud [4-8].

B. Reliability and Availability

Reliability and availability are two major factors for any technological efficiency. The availability of uninterrupted resources, the data loss or failure manipulates the reliability. The cloud computing is mostly affected by down time. Redundant resources utilization can be done to achieve the reliability. The risks can be denial of service attacks, performance slowdowns, resource outages and natural disaster.

In order to remove uncertainty and disinformation, the reliability, availability and security are the important and prime concerns to an organization. These concerns must be considered carefully while planning, developing and deploying the cloud set up for an organization so that consumers are provided with effective and secured services [9].

C. Performance

The cloud must provide improved performance which is expected by a user while moving from conventional architecture to cloud. Performance is measured by the application running on the cloud system. Performance is based on resources like disk space, CPU speed, memory, bandwidth, Network connection speed etc. Poor performance can result in loss of customers, improper services delivery, reduction is revenues, etc. [1, 5, 7].

D. *Interoperability and Portability*

Interoperability is the ability to use the same applications, modules and services across various cloud service providers platforms. Users must have freedom and flexibility to switch from one cloud to another without any restriction from the vendor as and when a user wants. The main concern is lack of standards, open APIs, lack of standard interface for virtual machines, deployment interfaces for services. Cloud portability ensures that one solution will be able to work with other platforms, applications and services as well [8].

E. *Scalability and Elasticity*

Scaling and extension are important factors while deployment of any technology and cloud remains no exception. Scalability can be defined as the ability of the system to perform well even when the resources have been added up. Elasticity means that the allocation of resources can get bigger or smaller depending on the requirement. This process of allocation is dynamic. Elasticity enables scalability. The scalability can be vertical or horizontal, where vertical scalability refers to addition of resources like memory or process to the single node in the system and horizontal scalability means addition of more nodes, like computer, to the existing system [9].

F. *Resources Management and Scheduling*

The resources management includes memory management CPU, Disk space, Input-output devices, and virtual machines. The efficient allocation and provisioning of resources provides high performance and higher service level. The scheduling can be done for resources provisioning so that out of various jobs and process, the priority can be assigned to jobs and sequencing can be done for systematic execution. It also deals with load balancing, resources management, synchronization, process pre-emption, pre-processing requirements, etc. The proper management and scheduling of resources will minimize the wastage and maximize the quality of services (QoS) standards.

G. Bandwidth Cost

While working on cloud, the uninterrupted high speed communication channel is of prime importance. To use the complete infrastructure of the cloud setup, it is required that high speed links must be provided for continuous data movement, resources sharing and security.

The clouds store consumer’s data which has its related concerns. The security measure must be taken into account for the sensitive data movements among users and various clouds increase the cost of data communication when more than tone cloud is involved (private/public/hybrid).

H. Virtualization

Virtualization is incorporated to obtain increased performance from the cloud computing. Virtualization also helps in providing benefits to users like cost effectiveness, simplified remote access, increased performance, infrastructural independence, scalability and elasticity, etc. However, Virtualization also leads to complex infrastructure which is difficult to manage and deploy. Therefore to implement and manage it, highly automated processing is required which increases the overhead.

IV. VARIOUS SECURITY THREATS

According to a report from the *Cloud Security Alliance*, here are the biggest security threats of cloud computing [10]:

A. Data Breaches

A data breach might be the main objective of a targeted attack resulting from human error, application exposures, or poor security structure. It might involve unintended public disclosure of personal information and may lead to data loss. A strong authentication and authorization process at various levels of access permissions may be included to handle it.

B. Deficient Identity And Access Supervision

Attackers acting as valid users, operators, or developers can read, modify, and delete data; sneak on data in transit or trigger malicious software that seems to originate from an authentic source resulting into unauthorized access to data and potential damage to organizations’ and its users’ data.

C. Insecure Application Programming Interfaces (APIs) Implementations

Software that customers use to manage and interact with cloud services perform management and monitoring with the User Interfaces (UIs) or APIs, and the security and availability of overall cloud services depends on the security of APIs. They need to be designed to defend against accidental and malicious attempts to privacy invasion.

D. Service Hijacking

Service hijacking leads to eavesdropping on actions and transactions of services, usage and modifications on data. Attackers can make frequent access to critical areas of cloud computing services with the stolen credentials, allowing them to negotiate the privacy, integrity and availability of the services.

E. System Vulnerabilities

Attackers can use bugs in programs to infiltrate a system to steal data or interrupt the services. Vulnerabilities within the components of the system put the security of all services, resources and data at substantial risk. Development of multi-tenancy in the cloud lead the systems from various organizations to be placed close to each other and given access to shared memory, data, services and resources.

F. Malicious Insiders

A malicious insider such as a system administrator can access potentially sensitive information, and can have increasing levels of access to more critical systems and eventually to data. Systems that depend solely on cloud service providers for security are at greater risk.

G. *Data Loss*

Permanent loss of customer data can happen due to an accidental deletion by the cloud service provider or a physical catastrophe such as a fire or earthquake. The provider or cloud consumer must take suitable measures to back up the data for disaster recovery and loss prevention.

H. *Denial Of Service (DoS)*

A DoS attack is designed to prevent cloud omputing service or resource from providing its normal services for a period of time. Such attacks cuts the availability of the cloud resources and services as a result handling the valid user requests becomes problematic.

V. CONCLUSION

Cloud computing has been and will be an integral part of organization, ranging from small –sized to large sized. Many organizations have already implemented the cloud computing to boost the quantity and quality of their services, to increase the users over internet and lower down the cost involved. Consumers also benefit from the pay per use criteria as they only have to pay for the resources that they use. Irrespective of high prospects it provides for business, organizations and researchers, it has various challenging issues which require serious consideration while exploring and using this technology like security, privacy, availability, performance, resource management, scalability etc.

This paper has discussed the cloud computing concepts and some challenges along with security threats attached with the technology. Cloud security has to be a part of an organization's overall security strategy. Organizations that rush to implement cloud technologies and choose providers without carrying out due diligence, expose themselves to a number of risks. Therefore, efficient evaluation of the technologies and the providers is crucial for the highest chance of success. While security patches are becoming available that only make it harder to execute an attack but they might also degrade the system's performance. There can be a few more challenges which require more in-depth analysis like automation management rules and policies for switching between clouds, cost model, advanced resources management and virtualization implementation factors. The further research on the cloud computing challenges and security threats will lead to its higher adoptability, acceptability and performance up-gradation.

REFERENCES

[1] IBM, Google and IBM announced university initiative to address internet-scale computing challenges, October-2007.

[2] S. Lohr, Google and I.B.M. join in Cloud computing research, October-2007.

[3] IBM, "IBM introduces ready-to-Use Cloud computing", November-2007

[4] L. Badger, T Grance, R. P. Comer and J. Voas, DRAFT cloud computing synopsis and recommendations, Recommendations of National Institute of Standards and Technology (NIST), May-2012.

[5] Y. Ghanam, J. Ferreira and F. Maurer, "Emerging issues & challenges in Cloud- A hybrid approach", Journal of software engineering and applications, vol. 5, no. 11, pp. 923-937, November 2012.

[6] M. A. Vouk, "Cloud computing – Issues, research and implementations", Journal of computing and information technology, Vol. 16, no. 4, pp. 235-246, June- 2008.

[7] T. Dillon, C. Wu and E. Chang, "Cloud computing: Issues and challenges", 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 27- 33, 2010.

[8] European CIO Cloud Survey, Addressing security, risk and transition, May -2011.

[9] G. T. Lepakshi, "Achieving availability, elasticity and reliability of the data access in cloud computing", Int. journal of advanced engineering sciences and technologies, vol 5, no. 2, pp. 150-155, April 2011.

[10] https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html accessed on March 05, 2018.