Cloud Security: A Concerning Issue

Apurva Aggarwal*
Shalini Sharma**

Abstract

Cloud computing is defined as an architecture which provides computing services by the use of internet on demand and we pay per use on having the access to a pool of shared resources like storage, servers, applications, services and networks and there is no need to physically possess them. So by this the time of the organizations and the cost for managing can be saved. The organizations and some of the industries like education, healthcare and banking are shifting towards the cloud as the services which are offered by the pay-per-use pattern which are based on the resources such as bandwidth consumed, amount of data transferred, processing power or the amount of storage space occupied etc are more efficient . Cloud services are delivered by data centres which are located all over the world. Cloud computing is a totally internet dependent technology in which the client data is stored and is maintained in the data centres of the cloud provider like Amazon, Google and Microsoft etc.

Keywords: quantum cryptography.

Introduction

Cloud refers to a network or Internet .Or we can say in other words as something which is present at remote location is cloud. Cloud computing provide us a way to have access over the applications as utilities, over the Internet. Cloud computing provides the creation, configuration and customization of applications online.Cloud computing ease its consumers by giving them virtual resources by means of internet. The fast growth in field of "cloud computing" also gives rise to severe security concerns. Security issues persist for Open Systems and internet. Cloud computing has not been widely adopted due to lack of security. Cloud computing have security issues like data securing, examining and analysing the usage of cloud by the cloud computing vendors. Both Cloud service provider and the cloud service consumer needs to make sure that the cloud is secure from all the external threats so that the customer does not face any problem like data loss or theft of data. A possibility also exist where a malicious user can access the cloud by impersonating as a legitimate user, and thus infecting the entire cloud and somehow affecting many customers who are sharing that infected cloud.[1]

Apurva Aggarwal*
Management Education & Research Institute
Shalini Sharma**
Management Education & Research Institute

Models

In cloud computing, the working models are deployment model and service model.

The type of access given to the cloud is defined by Deployment model. Different types of accesses that a cloud can have are: Private, Public, Hybrid, and Community.

Private cloud: Because of its private nature it offers more security .By the help of private cloud the system and the services are accessible within an organization.

Community cloud: The system and services are made to be accessible by the group of organizations.

Public cloud*:* System and services are made accessible to the general public. Its less secure as they are open that is free unrestricted access of the information.

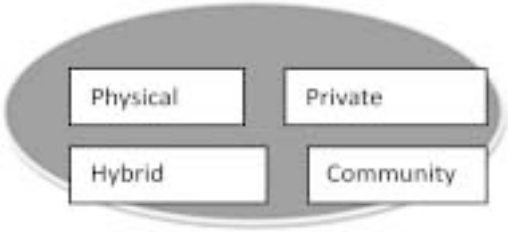

Figure 1: Different Accesses Given to Cloud

Hybrid cloud*:* It is a mixture of public and private cloud. All the critical activities are carried out by using private cloud and all the non-critical by using public cloud.

Service model: The cloud computing is based are called as Service models. It can be categorized into three service models as:

1) IaaS- Infrastrucure as a Service
2) PaaS-Platform as a Service
3) SaaS-Software as a Service

Infrastructure as a Service (IaaS) is the basic level of service. IaaS gives grant to fundamental resources like physical machines, virtual storage, etc.

PaaS-The runtime environment for applications, development and deployment tools are made available by PaaS.

SaaS-This model helps to have the Software applications being used as service to end users.

Popular Services for Cloud Computing are:

- **iCloud**. Apple's iCloud allows you to store music, documents, photos, and other files through Wi-Fi. And is accessible from any of your devices. By signing up for iCloud, you get 5GB of free storage automatically. For add on storage: $20 per year for 10GB, $40 per year for 20GB, and $100 per year for 50GB. All the other Apple apps (calendar, mail, and more) are combined to work effortlessly with iCloud.
- **Google Cloud.** It includes sharing data and editing data of Word, PowerPoint, and Excel. You can have secured copies of each document which is saved. This plan can be terminated at any time, price at $5 per user account per month, while the annual plan is priced at $50 per user account per year.
- **IBMSmartCloud**: it provides many services for the companies in IT sector, such as applications developed in the cloud or using the cloud as a backup for the company data. Use the price estimation to estimate the cost for your particular needs – hence you need to therefore select the software, its size, and times that you want to use, and any additional requirements that your company might contain. A 12-month commitment, for example, is at price $1,300 per month for each unit. [2]

Security Issues Cloud Computing:

The security for cloud and non-cloud are almost similar. The Cloud Security Alliance's initial report contains a different sort of log based on different security domains and processes which are needed to be followed in general cloud operations. Some privacy and security-related issues that are believed to have long-term implication for cloud computing are:

A. Governance

Governance implies management and drop by the organization on procedures, standards and policies for application development and data technology service attainment, also because the style, execution, testing, use, and watching of deployed or engaged services.

B. Compliance

Compliance refers to an association's responsibility to work in the favor of established laws, provision and standards. One with all the common compliance problems facing a company is information location means storage of data or information [3].

C. Malicious Insiders

This threat is well known to most of the organizations. Insiders who are malicious they put an impact on the organization which is considerable. The nasty insiders are the threat which has access to the data or information about the organization who are the members. The application made for cloud consumers allows the data to be stored on cloud provided by cloud provider which also has the access to that data too.

D. Account or service Hijacking

The reason for this threat is due to spoofing, spuriousness and vulnerabilities in the software. In this way the criminal can get access to critical information stored on the cloud from where he can take permission and steal up the data, leading to the compromise on the availability, probity, and confidentiality to the services available.

E. Hypervisor vulnerabilities

The Hypervisor is the main software component of Virtualization. There known security susceptibility for

hypervisors and solutions are still limited to an extent and often proprietary.

F. Insecure APIs

Anonymous access, reusable tokens or password, clear-text attestation or transmission of content, inflexible access controls or improper authorizations, limited auditing, and classification capabilities etc security threats may occur to organizations if the weak set of interfaces and APIs are used.

Our Recommendation

In this paper we will like to propose our ideas for future implementation:

The idea of "Quantum cryptography"should be applied to reduce challenges faced in security of data in cloud computing. Further research in this method's application is still going on in China. We are still further working on this direction[4].

Some of the goals to provide data securism include three major points. namely: Availability, secrecy, and authenticity. Confidentiality of data in the cloud is obtained through cryptography.

Quantum cryptography can be considered for future implementation. But unlike, the traditional **cryptology** methods as encoding and decoding the information, Quantum cryptology depends on physics not on mathematics[5],[6].

Quantum cryptography, a method used for transmitting a secret key over a distance which is secured and is based on the laws of physics. Quantum Key Distribution uses quantum mechanism to ensure secured communication[7]. It allows two parties to generate a random shared secret key which is known only to them and can be used to encrypt and decrypt

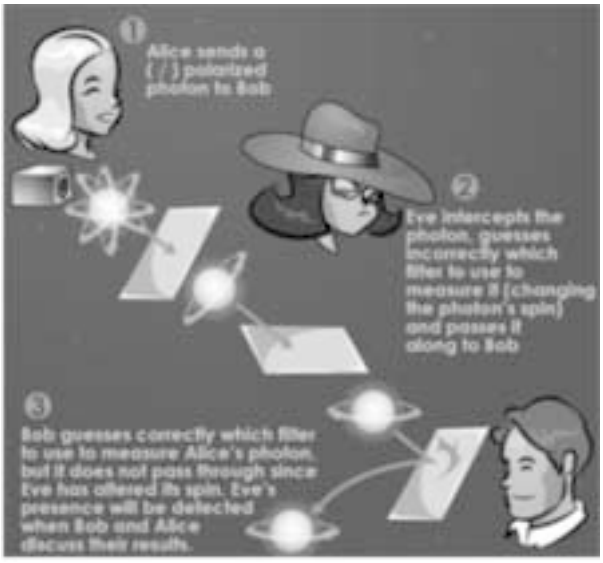

Figure 2: example for detection

the information. In quantum computing, a quantum bit is a unit of quantum information. The state of a qubit can be 0 and 1 simultaneously[8]. Explanation, consider a qubit be a single photon and see how it can be manipulated in the diagram below.

(a) 1st a photon emitted from a light source and passes through a linear polarizer, horizontally. This creates a qubit with horizontal polarization.

(b) When the photon which is polarized horizontally passes through a horizontal/vertical oriented beam splitter which is also polarised, then it always retains its horizontal polarization.

(c) Suppose that photon which is horizontally polarized passes via diagonally oriented polarized beam splitter:

- Approximately 50% of the photons could be found at one of the exiting.

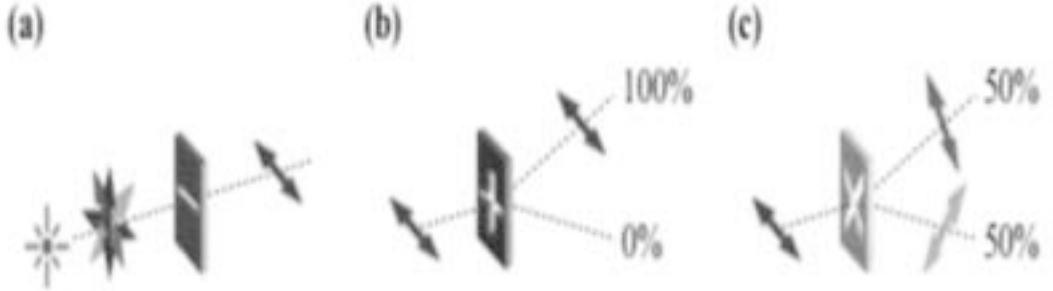

Figure 3: Manipulation of a Qubit

- The photon can only be detected at one of the existing.
- The polarization of the photon will change as per the corresponding diagonal polarization. Then Polarized photons are able to communicate digital information [9].

Conclusion and Future Scope

Modern cryptography algorithms are based on the fundamental process which includes finding factors of large integers into their primes, which is said to be ineradicable. But modern cryptography is susceptible to both technological progress of computing power and development in mathematics to quickly reverse one-way functions such as that of factoring large integers. So the idea is to introduce quantum physics into cryptography, which has lead to the evaluation of quantum cryptography. Quantum cryptography is one of the emerging topics in the field of IT industry. Hence quantum cryptography and how this technology contributes value to a defense-in-depth strategy related to completely secure key distribution is still in process.

References

1. Swaroop S. Hulawale, Cloud Security Using Third Party Auditing and Encryption Service , 5 june, 2013
2. http://talkincloud.com/
3. https://www.gov.uk/government/publications/implementing-the-cloud-security-principles/implementing-the-cloud-security-principles#audit-information-provision-to-consumers
4. http://searchsecurity.techtarget.com/definition/quantum-cryptography
5. https://sw.csiac.org/techs/abstract/520602
6. http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm
7. https://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf
8. http://www.sans.org/reading-room/whitepapers/vpns/quantum-encryption-means-perfect-security-986
9. http://www.wired.com/2013/06/quantum-cryptography-hack/