Security Concerns in Cloud Computing

Anu Gupta
Department of CSE, Kurukshetra Institute of Technology and Management (KITM)
Kurukshetra, INDIA
annugupta002@gmail.com

Abstract **- Now a days cloud computing can be viewed as a Buzzword. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Although there are several advantages of cloud computing, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which hamper the adoption of cloud computing. This paper introduces the detailed analysis of cloud computing security issues and challenges focusing on cloud computing types and service delivery types. This paper mainly purposes the core concept of secured cloud computing.**

Keywords **- cloud computing, cloud security, security issues, security Techniques**

I. INTRODUCTION

U.S. National Institute of Standards and Technology (NIST) [1] defines Cloud computing as "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". This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. Cloud computing lets you access all your applications and documents from anywhere in the world, freeing you from the confines of the desktop and making it easier for group members in different locations to collaborate. Moving data into cloud offers great convenience to users since they don't have to care about the complexities of hardware management. [2] defines cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Different researchers describe cloud computing in different ways. Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data [3]. Cloud computing provides different services and these services are available into three models.

A. Cloud service models

1) *Software as a Service (SaaS):* It is mostly run by cloud service providers to the organizations and users can access this from the internet.

2) *Platform as a Service (PaaS):* It is a tool for developing the websites without installing any software on the system and without the administrator rights.

3) *Infrastructure as a Service (IaaS):* It is controlled and maintained through various cloud services providers and can perform task such as storage, hardware, networking and servers.

B. Cloud deployment Models

There are different types of clouds which can be categorized as follows:

1) *Public cloud:* This cloud infrastructure is available only for public or a large industry group and it is provided by single service provider selling cloud services like Google App engine or Amazon elastic cloud compute offer its users highly flexible cloud environment. They enable users to share and store data as per their personal capacities.
2) *Private cloud:* It is generally operated by an organization and its main benefit is security and integrity of data.
3) *Hybrid cloud:* This architecture is a mixture of two or more clouds. It helps in load balancing between the clouds.
4) *Community cloud:* This model contains features of both the public and private cloud models. It is operated by organizations of a specific community.

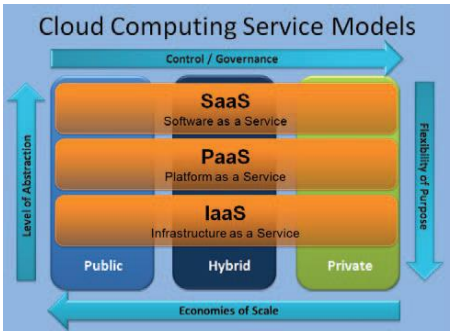

Fig. 1 cloud deployment model-service and delivery

In this paper different security issues involved in the cloud computing is analyzed. This research should help cloud consumers and providers to have an insight to understanding of the cloud security issues. This paper is organized as follows. Section 2 explores the cloud data security. Section 3 explores the major security issues from different perspectives. Section 4 outlines the different security techniques. Finally section 5 concludes the paper with future work.

II. CLOUD SECURITY

Security has emerged as the most important barrier to faster and widespread adoption of virtualization as well as cloud computing. It depends from person to person as well as industry to industry how they analyze the concept of security in Cloud Computing. The main questions while shifting to cloud are:

1. How secure is the data?
2. Where is the data?
3. Who has access?
4. Can you trust the company or third party?
5. How much confidential will your data be?
6. How does cloud provider keep different clients data separated and inaccessible from other clients?

In cloud [6], users do not know what position the data and do not know which servers are processing the data. The user do not know what network are transmitting the data because the flexibility and scalability of cloud system. The user can't make sure data privacy operated by the cloud in a confidential way. The cloud system can deploy the cloud center in different area and the data can be stored in different cloud node. There are various attacks that may be posed by attackers as cloud computing and web services run on a network structure so they are open to network type attacks. One of these is the distributed denial of service attacks. If a user could hijack a server then the hacker could stop the web services from functioning and demand a ransom to put the services back online. To stop these attacks the use of syn cookies and limiting users connected to a server all help stop a DDOS attack. Another such attack is the man in the middle attack. If the secure sockets layer (SSL) is incorrectly configured then client and server authentication may not behave as expected therefore leading to man in the middle attacks. It is clear that the security issue has played the most important role in hindering Cloud computing. Without doubt, putting your data, running your software at someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues are described in section 3.

III. CLOUD SECURITY ISSUES

For analysis of cloud computing security issues we concentrate on the following key research areas:

a) Multi-tenancy
b) Elasticity
c) Network insecurity
d) Location based
e) Virtualization
f) Vendor lock-in

a) Multi-tenancy: Multi-tenancy implies sharing of computational resources, storage, services and applications with other tenants, residing on the same physical or logical platform at the provider's premises. Multiple tenants [5] share the same physical or logical access, storage, database, memory and other resources in cloud paradigm as shown in fig. 2. This sharing of resources violates the confidentiality of tenants' IT assets which lead to the need for secure multi-tenancy. This implies that unless there's degree of isolation between these tenants, it is very difficult to keep an eye on the data flowing between different realms which inherently makes multi-tenancy model insecure for adoption.

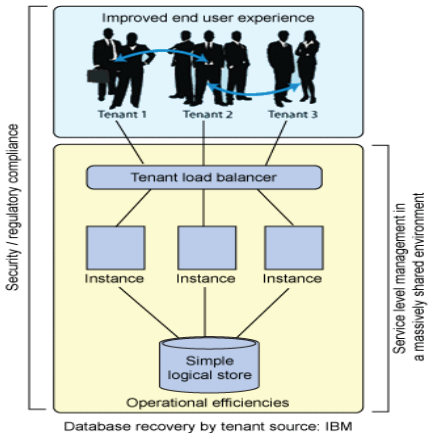

Fig. 2: Cloud Multi-Tenancy model

b) Elasticity: Elasticity is another important aspect of cloud computing and implies that consumers are able to scale up or down resources assigned to services or resources based on the current demand shown in fig.3. Different users uses same machine to run their application using virtualization technique. This may lead to data breach. For example, a tenant scaled down and released resources which are now assigned to another tenant who in turn now uses it to infer the contents of previous tenant. This can be extremely unacceptable to an organization or business as its data information is exposed and it can lose business.

*c) Network insecurity***:** The amount of traffic and uncontrolled nature of network may lead to data loss.

d) Location Based: As the Cloud clients are not sure of the location of their data raises the insecurity of the data. In cloud clients are unaware of the location of their stored data. As in cloud, provider has the complete hold on data it may lead to loss of data [4].

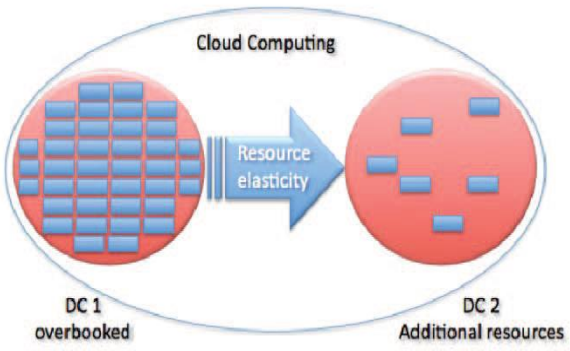

Fig.3. Cloud resource Elasticity

e) Virtualization: The cloud computing runs on the technique of virtualization where same system is allocated for multiple users at the same time there are possibilities that lead to unsafe of data.

f) vendor lock-in: The problem of vendor lock-in [7] should be handled .It implies if a company is dissatisfied with one cloud computing service- or if the vendor goes out of business- the firm cannot easily and inexpensively transfer these services to another provider or bring it back in-house.

Apart from these there are several other issues from different perspective.

A. Service Provider Security issues

- *Privacy:* Privacy is the one of the Security issue in cloud computing. The data which is stored on cloud should be kept private from other clients or organizations to prevent it from changes by other entity.
- *Securing Data in Transmission*: Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. In Cloud environment most of the data is not encrypted in the processing time, but to process data, for any application that data must be unencrypted. In fully homomorphism encryption scheme advance in cryptography, which allow data to be preprocessed without being decrypted.
- *User Identity:* In Organizations, only authorized users across their enterprise and access to the data and tools that they require, when they require them, and all unauthorized users are blocked for access. In Cloud environments support a large enterprise and various communities of users, so these controls are more critical. Clouds begin a new level of privileged users working for the cloud provider is administrators. And an important requirement is privileged user monitoring, including logging activities. This monitoring should include background checking and physical monitoring.

B. Infrastructure Security Issues

From infrastructure perspective there are several issues which are given as:

- *Securing Data-Storage:* In Cloud computing environment data protection as the most important security issue. In the service provider's datacenter, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self encrypting is used by hard drive manufacturers.
- *Network and Server (Server-Side Protection):* Virtual servers and applications, very like their non-virtual counterparts, have to be compelled to be secured in IaaS clouds, each physically and logically. Example, virtual firewalls are often used to isolate teams of virtual machines from different hosted teams, like production systems from development systems or development systems from different cloud-resident systems.

C. End User Security Issues

- *Browser Security*: In a Cloud environment, remote servers are used for computation. The client nodes are used for input/output operations only, and for authorization and authentication of information to the Cloud a standard Web browser is used. Platform independent client software useful for all users throughout the world. This can be categorized into different types: Software as- a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryption and host authentication.
- *Authentication and data integrity*: In the cloud environment, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Authentication is necessary to protect the data from unauthorized users. Data Integrity is another important security issue which implies data should not be altered stored on cloud by any unauthorized entity.
- *Data protection:* cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g. between federated clouds.

IV. SECURITY TECHNIQUES USED IN CLOUD COMPUTING

Various security techniques used by cloud computing providers to secure the transmission of data between cloud and LAN are:

- *Public Key Cryptography*: To resolve problem regarding authentication and integrity in cloud computing over users data implement Public key cryptography over cloud is best answer. When transmission of data occurs between users and cloud then a lot of problems occurs due to an attackers or unauthorized users access. The confidential data will be treated outer people of company and the other people can access the data .To solve data security related problems cloud provider must use the public key cryptography concepts. The data can be encrypted before stored in the cloud system. This technique can protect user data privacy and security in cloud the environment to some extent.
- *Access Control Policy:* Access control policy is basic technology and is to ensure that network resources are not illegal use. It includes network access control and directory level security control. The user which can connect the cloud system includes the cloud provider, operation and maintenance personnel and the customer user.
- *Secure Socket Layer(SSL):* SSL is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. SSL protocol determines variables of the encryption for both the link and the data being transmitted.
- *Third Party Auditor:* TPA is the third party auditor who will audit the data of data owner or client so that it will let off the burden of management of data of data owner. TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. It reduces the communication overhead for the client as it is responsible for the verification of data.

V. CONCLUSION

The cloud computing phenomenon is generating a lot of interest worldwide because of its lower total cost of ownership, scalability and flexibility, reduced complexity for customers, and faster and easier acquisition of services. Despite of these advantages several consumers don't want to store data on cloud because of the security problem. This paper explores the security issues at various levels of cloud computing service architecture. Security of consumer information is a major requirement for any services offered by any cloud computing. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Various security techniques to tackle these issues also proposed. To gain the total acceptance from the users, enterprises effective security techniques are required to solve these security issues.

REFERENCES

[1] Peter Mell, Timothy Grance " *The NIST Definition of Cloud Computing*", Special Publication 800-14

[2] Shaik Khaja Mohiddin, Md. Khamr-uddin, K Mohan Krishna, *An Overview of Data Security in cloud computing*, Int. J. of advances in computer, Electrical & Electronics Engg., Vol .2, pp. 37-42, 2012.

[3] Mrs. Aarti P. Pimpalkar, Prof. Hingoliwala H.A., *Ensuring Data Security in Cloud Computing*, pp. 129-132, 2013.

[4] V. Nirmala, R.K. Sivanandhan, Dr. R.Shanmugalakshmi, *Data Confidentiality and integrity verification Using User Authenticator Scheme in Cloud*, IEEE/ICGHPC 2013.

[5] Akhil Behl, Kanika Behl, *An analysis of cloud computing security issues*, pp.109-114, 2012, IEEE.

[6] Wentao Liu, *Research on cloud computing security problem and strategy*, 2012 IEEE.

[7] Rajendra Kumar Dwivedi, *From grid computing to cloud computing and security issues in Cloud computing*, vol. 5, july 2012.

[8] Anu Rathi, Yogesh Kumar, Anish Talwar, *Aspect of Security in Cloud Computing*, IJECS, Volume 2, Issue 4, April 2013.

[9] Ertaul, S. Singhal, G Saldamli, *Security Challenges In Cloud Computing*.

[10] Karamjit Singh, Isha Kharbanda, Navdeep Kaur, *Security issues occur in Cloud Computing and their solutions*, IJCSE, Vol. 4, May 2012.

.