A Study of Cloud Security: challenges and Concerns

Subhash Singh Parihar
Director, Prabhat Engineering College Kanpur (D)
Uttar Pradesh, INDIA

***Abstract*- "The cloud" refers to servers that are accessed over the Internet and the software and databases that run on those servers. The cloud has allowing users and organizations to rely on external providers for storing and processing their data and making them available to others. Cloud servers are located in data centres all over the world. Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. In this paper, we study of cloud security related to challenges and concerns. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access and an increasing important priority for the wide adoption and acceptance of cloud computing is the ability of data owners and users to have enforced and assess security guarantee. Cloud security is the protection of data, applications, infrastructures involved in cloud computing like any computing environment, involves maintaining adequate preventative protections and ensuring confidentiality and integrity of data, access, and computations on them as well as ensuring availability of data and services to genuine users and in compliance with agreements with the providers.**

Keywords- Cloud Security, Confidentiality, Integrity Availability, Cloud storage server, Data storage

I. INTRODUCTION

Cloud Computing offers many advantages such as increased utilization of hardware resources, scalability, reduced costs, and easy deployment. As a result, all the major companies including Google, Amazon and Microsoft are using cloud computing. Moreover, the numbers of customers moving their data to cloud services such as icloud, Google Drive, Drop box, Face book LinkedIn and many moiré increasing every day.

To control the security risks in cloud, it is crucial for researchers, developers, service providers, and users to understand them so that they can take maximum precautions, deploy existing security techniques or develop new ones. In this paper, the top security threats for cloud computing presented by Cloud Security Alliance (CSA) [1] have been analyzed.

Cloud Computing generally defined as an IT model or computing environment composed of IT component which commonly consists of hardware, software, network and services. [2]

The cloud computing model is most commonly composed of seven essential characteristics, three service models and four deployment models.

The seven essential characteristics are as follows:

1 On-demand self-service
2 Broad network access
3 Resource polling
4 Rapid elasticity
5 Measured service
6 Location Independence
7 Ubiquitous network access

The three service models are as follows:

1 Software as Service (SaaS) [3]-It uses provider's application over a network.
2 Platform as a Service (PaaS) [4]-Used for deploying customer-created applications to a cloud.
3 Infrastructure as a Service (Iaas) [5]-used for network capacity, rent processing, storage etc.

The deployment models can be either internally or externally implemented. These are commonly four different types of deployment models which are summarized in the NIST [6], [7] and are defined as follows: public infrastructure.

a) Public cloud-Sold to the mega-scale, use by the public .It may be owned, managed and operated by a business, academic or government organization.
b) Community cloud-Shared infrastructure for specific community[17]
c) Private cloud-Enterprise leased or owned and use by single organization comprising multiple consumers (e.g. business unit).
d) Hybrid cloud-composition of two or more clouds (private, community, or public).

This paper is composed as follows: Section II describes the most critical threats for cloud computing and their effects on cloud entities

II. CLOUD COMPUTING SECURITY CHALLENGES

The biggest challenge in achieving cloud computing security is to keep data secure. The major issues that arise with the transfer of data to cloud are that the customers don't have the visibility of their data and neither do they know its location. They need to depend on the service provider to ensure that the platform is secure, and its implements necessary security properties to keep their data safe.

According to Nathan Eddy in the article named "Security a Rising Concern for Cloud-Based Application Usage" a survey was conducted which indicated that unsafe password management continues to be a challenge, as is the application usage which is not sanctioned by the company **[8].**

Here is the list of various security threats found in cloud computing:-

1. **Data Breaches:** Data Breaches are one of the top threats to cloud computing. Data breach is defined as the leakage of sensitive customer or organization data to unauthorized user. It can occur as the attacks by malicious users who have a virtual machine (VM) on the same physical system as the one they want to access in unauthorized way.
2. **Data loss:** Data loss is the second most important issue related to cloud security. Data loss mostly occurs due to malicious attackers, data deletion, data corruption, loss of data encryption key, faults in storage system, or natural disasters.44 percent of cloud service providers have faced brute force attacks in 2013 that resulted in data loss and data leakage[9].
3. **Denial of Service :** Denial of service (DOS) attacks are done to prevent the legitimate users from accessing cloud network, storage, data, and other services.DOS attacks have been on rise in cloud computing in past 5 years and 81 percent customers consider it as a significant threat in cloud[1].
4. **Malicious insiders:** A malicious insider is someone who is an employee in the cloud organization, or a business partner with an access to cloud network, applications, services, or data misuses his access to do unprivileged activities. Cloud administrators are responsible for managing, governing, and maintaining the complete environment. They have access to most data and resources, and might end up using their access to leak that data. Other categories of malicious insiders involve hobbyist hackers who are administrators that want to get unauthorized sensitive information just for fun, and corporate espionage that involves stealing secret information of business for corporate purposes that might be sponsored by national governments.[10]
5. **Cloud environment specific threats:** Cloud service providers are largely responsible for controlling the cloud environment. However, a survey report by Alert Logic [9] shows that almost 50 percent of the cloud users consider service provider issues as a major threat in cloud computing.
6. Insufficient due diligence:
7. Technology vulnerabilities
8. Traffic hijacking:
9. Insecure interfaces and API's

III. CHARACTERISTICS OF CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) **[14]** defines the cloud model is composed of five essential characteristics.

A. **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

B. **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

C. **The provider's computing res.:** Resource pooling sources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data enter). Examples of resources include storage, processing, memory, and network bandwidth.

D. **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

E. **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

IV. CLOUD SERVICE DELIVERY MODEL

The National Institute of Standards and Technology (NIST) **[14]** define three Cloud Service Delivery Models.

A. **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

B. **Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

C. **Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing

resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

V. CLOUD DEPLOYMENT MODELS

Regardless of the service model utilized (SaaS, PaaS, or IaaS), there are four deployment models for cloud services with derivative variations that address specific requirements. It is important to note that there are derivative cloud deployment models emerging due to the maturation of market offerings and customer demand. An example of such is virtual private clouds — a way of utilizing public cloud infrastructure in a private or semi-private manner and interconnecting these resources to the internal resources of a consumer's data enter, usually via virtual private network (VPN) connectivity.

A. Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

B. Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

C. Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

D. Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

VI. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY IN THE CLOUD

Confidentiality requires guaranteeing proper protection to confidential or sensitive information stored or processed in the cloud. for ensuring confidentiality, cryptographic encryption algorithms and strong authentication mechanism can be used .Integrity requires guaranteeing the authenticity of: the parties (users and providers) interacting in the cloud, the data stored at external providers, and of the response returned from queries and computations. Availability requires providing the ability to define and verify that providers satisfy requirements expressed in Service Level Agreements (SLAs) established between data owners/users and providers. The issues to be tackled, the challenges to be addressed, and the specific guarantees to be provided for ensuring satisfaction of the security properties above depend on the characteristics of the different scenarios.[10]

VII.SECURITY IN CLOUD ENVIRONMENT

In cloud computing paradigm, a cloud provider creates, deploys and manages the resources, application and services. Multi tenancy and virtualization are the key features to make efficient utilization of the existing resources and application. A single server, computing facility, data centre and operating system hosts many users, using virtualization. A large number of users are getting served by a cloud provider by this concept of resources sharing. Data protection, communication, resource management for isolation, virtualization etc. are some of the security issues arises due to multi-tenancy and virtualization in the cloud environment. Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions [12]

An organization's security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), and all the way to the information and applications (application security). Additionally, controls are implemented at the people and process levels, such as separation of duties and change management, respectively [11].

A. Data Protection: The cloud computing infrastructure is shared among multiple users at any point of time. User data is stored and processed in the shared environment in a cloud that is under provider's control. User data may be tampered by other malicious entity in the cloud. Lack of transparency about the data storage location in the cloud environment, regulatory issue due to cross border storage etc. makes the requirement of data privacy and protection in cloud environment more prominent.

B. Application Security: Application software running on or being developed for cloud computing platforms presents different security challenges. It is depending on the delivery model of that particular platform. Flexibility, openness and public availability of cloud infrastructure are threats for application security. The

existing vulnerabilities like Presence of trap doors, overflow problems, poor quality code etc. are treats for various attacks. Multi-tenant environment of cloud platforms, the lack of direct control over the environment, and access to data by the cloud platform vendor; are the key issues for using a cloud application. Preserving integrity of applications being executed in remote machines is an open problem.

C. **Network Security:** A cloud computing can be of type public or private depending on the accessibility of services. Service and applications are accessed from remote locations in a cloud environment. Continuous availability of cloud service without any disruption, denial of service, and other attacks are network security issues. Also Distributed Denial of Service, Signature wrapping attack etc. creates data transmission risks in the cloud network. The virtualization technology has severe impact on network security. Invisible network created by virtual servers makes it difficult to monitor network traffic and performance. Standard network security controls are not sufficient to control VM traffic and their job monitoring. Lack of robust sniffer, tracking and firewalling tools for virtualized network makes it difficult to achieve a secure network.

D. **Virtualization Security**: Virtualization technology introduces new attacks with the hypervisor and other management components. Multi-tenancy in cloud infrastructures for sharing physical resources between VMs (Virtual Machine), can give rise to man in the middle attack at the time of authorization for any service. VMs are created and revert back as and when needed in the cloud environment. Because VMs can quickly be reverted to previous instances, and easily moved between physical servers, it is difficult to achieve and maintain consistent security.

E. **Identity Management**: Identities are generated to access a cloud service by the cloud service provider. Each user uses his identity for accessing a cloud service. Unauthorized access to cloud resources and applications is a major issue. A malicious entity can impersonate a legitimate user and access a cloud service. Many such malicious entities acquire the cloud resources leading to unavailability of a service for actual user. Also it may happen that the user crosses his boundary at the time of service usage in the cloud environment. This could be in terms of access to protected area in memory or performing any other operation that are not maintained in Access control List for a specific resource and application. Thus Identity Management system for providing authentication and authorization is an issue for both provider as well as user in a cloud computing environment [13].

VIII. SECURITY CHALLENGES FACED BY CLOUD COMPUTING

The Cloud Security Alliance (CSA) survey identified 6 primary issues holding back cloud adoption, summarized below, and starting with the most common issues:

A. **Security of data** – It's no surprise that data security tops the list of concerns that hold companies back from cloud adoption. 73% of survey respondents indicated this is a big red flag for them [15]. Cloud service providers are targets data breaches (e.g. email service Send Grid (SendGrid is a cloud-based email service that provides reliable transactional email delivery, scalability, and real-time analytics along with flexible APIs that make custom integration easy**.** [13]

B. **Non-compliance with regulatory mandates** –The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept process, store or transmit credit card information maintain a secure environment.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) mandates audits of health care providers to investigate and determine if they are in compliance with the HIPAA Privacy Rule (effective in 2003) and Security Rule (effective in 2005).

The Gramm-Leach-Bliley Act (GLB Act or GLBA) is also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information.

The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. Whatever the regulatory acronym, you will find that 38% of companies are concerned with how they can assure compliance with regulations if their data is in the cloud.

A security breach that leads to non-compliance with a regulatory mandate can result in expensive fines, loss of business, lawsuits, and potentially even criminal penalties. If an exporter makes a factual omission of material information (or otherwise misrepresents facts) at any point in the registration, licensing, or reporting processes, then civil and criminal penalties may apply).

C. **Loss of control over IT services** – 38% of the CSA survey respondents say their fear over loss of control keeps them from moving data into cloud-based applications [16]. This loss of control cam be manifested in numerous ways. The cloud service provider may choose how and where data is stored; how often it is backed up; which encryption scheme is used, if one is used at all; which of its employees have physical or virtual access to the data; and more. But even if the cloud service provider invokes feelings of total trust, the fact remains that the data owner is still liable for any data breach that might occur, and this

leaves more than a third of all companies doubtful to use cloud services.

D. Expertise of IT and business managers – 34% of companies aren't jumping on the cloud bandwagon because they believe the knowledge and experience of their IT and business managers are not aligned with the skill sets that cloud computing demands. For example, in addition to the technical knowledge a manager is expected to have, the person also needs financial literacy for a new computing model where services are rented, not owned, plus negotiation skills to drive a cloud provider's service-level agreement (SLA) to the company's benefit. [7]

E. Compromised accounts or insider threats – 30% of the CSA survey respondents are concerned about what would happen if their accounts held by a SaaS provider were to be compromised in some way, or if an insider with that provider did a little "extra-curricular activity" and poked around in private accounts.[12]

F. Business continuity and disaster recovery – What happens to a company if it loses all access to its IT infrastructure because its cloud provider has suddenly gone out of business? A company doesn't abdicate its obligation to do proper business continuity and disaster recovery planning just because it no longer operates the physical aspects of its IT infrastructure, but recovering data from a defunct cloud service – and finding an alternative home for that data – can be a huge challenge.

IX. CONCLUSIONS

With the rapid growth of cloud computing platforms and services, cloud security is becoming a key priority for all players (i.e., individuals, companies, and cloud providers). Today, cloud computing is clearly one of the most enticing technology areas of the current times due, at least in part to its cost-efficiency and flexibility. When thinking about solutions to cloud computing adoption problem, it is important to realize that many of the issues are essentially old problems in a new setting, although they may be more acute. In this paper, we presented A study of Cloud Security: challenges and Concerns, illustrating their impact on the confidentiality, integrity, and availability properties.

REFERENCES

[1] T.T.W.Group et al., "The notorious nine: cloud computing top threats in 2013 Cloud Security Alliance, 2013".
[2] J.R. Vic Winkler the Cloud Computing Security Techniques and Tactice", 2011.
[3] Amazon Elastic Compute Cloud web services, http://aws.amazon.com/eC2
[4] SalesForce Force.com Platform as a service, http://developer.force.com
[5] NetSuite SaaS portal, http://www.netsuite.com
[6] National Institute of Standards and technology (NIST), http://www.nist.gov
[7] NIST, Guidelines on Security and Privacy in Public Cloud Computing, http://csrc.nist.gov/ publications 2011/
[8] Nathan Eddy, "Security a Rising Concern for Cloud-Based application Usage", http://www.eweek.com/security/security-a-rising-concern-for-cloud-based-application-usage,January 2013.
[9] "Cloud security report spring 2014" https;//www.alertlogic.com/resources/cloud-security-report//
[10] M. Kazim, S.Y.Zhu "A survey on top security threats in cloud computing" in International journal of advanced computer Science and applications in vol.6, No.3, 2015.
[11] Cloud computing for e-governance. White paper, IIIT-Hyderabad, January 2010. Available online (13 pages).
[12] Cloud Security Alliance – CSA, Top Threats Working Group (2013). The Notorious Nine - Cloud Computing Top Threats in 2013.http://www.cloudsecurityalliance.org/topthreats.
[13] Cloud Security Alliance – CSA (2011). Security Guidance for Critical Areas of Focus in Cloud ComputingV3.0.http://www.cloudsecurityalliance.org/guidance/
[14] National Institute of standards and Technology (NIST), http://www.nist.gov
[15] Shaikh S., Sasikumar M. (2012) "Security issues in cloud computing: A survey in International journal of Computer application, volume: 44, No.19.
[16] Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in Proceedings of the 8th International Conference on Network and Service Management. International Federation for Information Processing, 2012, pp. 37–45.
[17] Ronald L.Krutz, Russell dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", July2010.