International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

# Exploring Security Risks in Cloud Computing

**Mr. MD SAHIL (Dept of MCA)**
**Under the Guidance of, Assistant Professor Mrs. Manisha Patil**
(Dept of MCA), Trinity Academy of Engineering, Pune, India

**Abstract:**

Cloud computing and education sounds ambiguous on the face of it. Naturally, it's because, very few individuals, publishers and users alike come from the education sector. Cloud computing has become one of the most interesting topics in the IT world today. Cloud model of computing as a resource has changed the landscape of computing as it promises of increased greater reliability, massive scalability, and decreased costs have attracted businesses and individuals alike. It adds capabilities to Information Technology's. Over the last few years, cloud computing has grown considerably in Information Technology. As more and more information of individuals and companies are placed in the cloud, there is a growing concern about the safety of information. Many Companies that are considered to be giants in software industry like Microsoft are joining to develop Cloud services.

Despite the hype about the cloud, customers are reluctant to deploy their business in the cloud. Security issues is one of the biggest concerns that has been affecting the growth of cloud computing .It adds complications with data privacy and data protection continues to affect the market. Users need to understand the risk of data breaches in the cloud environment. The paper highlights issues related to cloud computing.

Keywords - Cloud computing, Security and Privacy, Threats.

**Chapter I:**

**Introduction:**

Software Developers describe Cloud in a different way than a System Administrator, while a Database Administrator may have different definition. Cloud means a wide range of scalable services that users can access via an Internet connection. Providers like Microsoft, Amazon, Google and many more provide various cloud-based services for which users can pay on the basis of service subscription and consumption. Many providers offer a wide range of Cloud services like Messaging, Social Computing, Storage, CRM, Identity management, Content Management etc. Cloud computing is dependent on resource sharing. Using these internet enabled devices, cloud computing permits the function of application software. Cloud computing is also known as the cloud. Cloud computing serves a wide range of functions over the Internet like storage. Taking advantage of resource sharing, cloud computing is able to achieve consistency and economies of scale. Types of cloud computing can be classified on basis of two models. Cloud computing service models and cloud computing deployment models. It is a file backup shape.It also allows working on the same document for several jobs of different types. Cloud computing simplifies usage by allowing overcoming the limitations of traditional computer. Cloud computing also provides more agility because it allows faster access. These hosted services are normally separated into three broad categories:

Infrastructure-as-a-Service(IaaS), Platform-as-a-Service(PaaS) and Software-as-a-Service(SaaS).

A cloud service is used by clients as and when needed, usually on hourly basis. This pay as you go approach

has made the cloud flexible such that where end user can have services the way they desire at any point of time and the cloud services is entirely monitored by the provider. There are some of the basic security threats that have exploited the usage of Cloud Computing. An example of security threat is botnets, the use of botnets to spread spam and malware. Of the 761 data breaches investigated in 2010 by the U.S. Secret Service, almost 63% occurred at companies with 100 or fewer employees. And a 2011 survey by security systems provider Symantec Corp. around 2,000 plus small and midsize enterprises indicated that close to 73% had been breached by a cyber-attack. One of the best features of cloud computing is pay-as-you-go model of computing as a resource. This model of computing has enabled businesses and organizations in need of computing power to purchase as many resources as they need without the need to put forth a large capital investment in the IT infrastructure. Other advantages of cloud computing are scalability and increased flexibility for a relatively constant price.

Cloud is the new trend in the evolution of the distributed systems. The user does not need knowledge or expertise to control the infrastructure of clouds, it provides abstraction. Cloud providers deliver common online business applications which are accessed from servers through web browser.

## Chapter II:

## Cloud Computing Models Related Work:

Cloud hosting deployment models are classified by the proprietorship, size and access. It tells about the nature of the cloud. Most of the organizations are willing to implement cloud since it reduces the expenditure and controls cost of operation.

Research exploring the security implications of various cloud computing models and proposing strategies to mitigate risks associated with each model.

### 2.1 Cloud computing deployment models

#### 2.1.1 Public Cloud

It is a type of cloud hosting in which the cloud services are delivered over a network that is open for public usage. This model is actually true representation of cloud hosting. In this the cloud model service provider provides services and infrastructure to various clients. Customers do not have any control over the location of the infrastructure. There may be very little or no difference between public and private clouds structural design except the level of security that are offered for various services given to the public cloud subscribers by the cloud hosting providers. Public cloud is suited for business which require managing load. Due to the decreasing capital overheads and operational cost the public cloud model is economical. Dealers may provide the free service or license policy like pay per user. The cost is shared by all the users in public cloud. It profits the customers by achieving economies of scale. Public cloud facilities may be available for free an e.g. of a public cloud is Google.

#### 2.1.2 Private Cloud

It is also known as internal cloud. This platform for cloud computing is implemented on cloud-based secure environment and it is safeguarded by a firewall which is governed by the IT department that belongs to a particular corporate. Private cloud permits only the authorized users and gives the organization greater control over their data. The physical computers may be hosted internally or externally they provide the resources from a distinct pool to the private cloud services. Businesses having unanticipated or dynamic needs, assignments which are critical management demands and uptime requirements are better suited to adopt private cloud. In private cloud there is no need for additional security regulations and bandwidth limitations that can be present in a public cloud environment. Clients and Cloud providers have control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples is Eucalyptus Systems.

**2.2: Cloud computing service models**

**2.2.1: Software as a Service (SaaS)**

Software as a Service (SaaS) is growing rapidly. SaaS makes uses the web to provide applications which are managed by a third-party vendor and whose interface is accessed on the client side. SaaS applications can be run from a web browser without the need to download or installation, but these require plugins. The cloud provider provides the consumer with the ability to deploy an application on a cloud infrastructure. Because of this web delivery model SaaS removes the need to install and run applications on individual computers. In this model it is easy for enterprises to improve their maintenance and support, because everything can be managed by vendors: applications, runtime, data, middleware, OS, virtualization, servers, storage and networking. Popular SaaS services include email and collaboration, healthcare-related application. SaaS providers usually offer browser-based interfaces. APIs are also normally made available for developers. The key benefit of SaaS is that it requires no advance investment in servers or licensing of software. The application developer, have to maintain one application for multiple clients.

**2.2.2: Infrastructure as a Service (IaaS)**

Infrastructure as a Service, are used for monitoring, and managing remote datacenter infrastructures, such as compute (virtualized or bare metal), storage, Users can purchase IaaS based on consumption, similar to other utility billing. IaaS users have the responsibility to be in charge applications, data, runtime and middleware. Providers can still manage virtualization, servers, storage, and networking. IaaS providers offer databases, messaging queues, and other services above the virtualization layer as well.

**2.2.3: Platform as a Service (PaaS)**

Platform as a service (PaaS) is a kind of cloud computing services that provides a platform that allows customers to develop, run, and manage applications without the problem of building and maintaining the infrastructure. One need not be bothered about lower level elements of Infrastructure, Network Topology, Security all this is done for you by the Cloud Service Provider. With this technology, third-party providers can manage OS, virtualization, and the PaaS software itself. Developers manage the applications. Applications using PaaS inherit cloud characteristic such as scalability, multi-tenancy, SaaS enablement, high-availability and more. Enterprises benefit from this model because it reduces the amount of coding, automates business policy, and help in migrating applications to hybrid model.

**2.1.3 Hybrid Cloud**

It is a type of cloud computing, which is integrated. It could constitute an arrangement of two or more cloud servers, i.e. either of the combination of private, public or community cloud that is bound together but remain individual entities. Hybrid clouds are capable of crossing isolation and overcoming boundaries by the provider; therefore, it cannot be simply categorized into public, private or community cloud. It allows the user to increase the capacity as well as the capability by assimilation, aggregation and customization with another cloud package / service. In a hybrid cloud, the resources are managed either in-house or by external providers. It is an adaptation between two platforms in which the workload exchanges between the private cloud and the public cloud as per the needs and demand of organization. Resources which are non-critical like development and test workloads can be housed in the public cloud that belongs to a third-party provider. While the workloads that are critical or sensitive should be housed internally. Organizations may use the hybrid cloud model for processing big data. Hybrid cloud hosting has features like scalability, flexibility and security.

**Chapter III:**

**SECURITY ISSUES:**

Cloud service models not only provide different types of services to users but they also reveal information which adds to security issues and risks of cloud computing systems. IaaS which is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud. IaaS also enables

hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Multiple virtual machines are supported by IaaS, gives an ideal platform for hackers to launch attacks that require a large number of attacking instances. Loss of data is another security risk of cloud models. Data in cloud models can be easily accessed by unauthorized internal employees, as well as external hackers. The internal employees can easily access data intentionally or accidently. External hackers may gain access to databases in such environments using hacking techniques like session hijacking and network channel eavesdropping. Virus and Trojan can be uploaded to cloud systems and can cause damage. It is important to identify the possible cloud threats in order to implement a system which has better security mechanisms to protect cloud computing environments.
3.1Threats in cloud computing

### 3.1.1 Compromised credentials and broken authentication

Organizations/companies at times struggle with identity management as they try to grant permissions appropriate to the user's job role. They sometimes forget to remove user access when a job function changes or a user leaves the organization. The Anthem breach exposed more than 80 million customer records, was the result of stolen user credentials. Anthem had failed to deploy multifactor authentication, so when the attackers obtained the credentials, it was all over. Many developers have made the mistake of embedding credentials and cryptographic keys in source code and have them in public-facing repositories.

### 3.1.2 Data breaches

Cloud environments face many of the same threats as traditional corporate networks, but since a large amount of data is stored on cloud servers, providers have become an attractive target. The severity of the damage tends to depend on the sensitivity of the data that is exposed. Personal financial information grabs the headlines,but breaches involving government information, trade secrets can be more devastating. When a data breach takes place, a company may be subjected to legal action. Breach investigations and customer notifications can rack up significant costs indirect effects may include brand damage and loss of business can impact organizations future for years.

### 3.1.3 Cloud service abuses

Cloud services may be used to support activities like using cloud computing resources to break an encryption key in order to launch an attack. Examples of these attacks include launching DDoS attacks, sending spam and phishing emails. Providers need to recognize kind of abuse to recognize DDoS attacks and offer tools for customers to monitor the health of their cloud environments. Customers should make sure that providers offer them a mechanism for reporting abuse. Even though customers may not be direct prey for malicious actions, cloud service abuse can still result in unavailability of service and data loss.

### 3.1.4 DDoS attacks

DoS attacks have been around for a long time and have gained prominence again thanks to cloud computing because they often affect availability. Systems may run slow or simply time out. These DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. High-volume DDoS attacks are very common, but organizations should also be aware of asymmetric and application-level DoS attacks, which target Web server and database vulnerabilities. Cloud providers are better poised to handle DoS attacks than their customers. The key here is to have a plan to mitigate the attack before it occurs, so administrators have access to those resources when they need them.

### 3.1.5 Account hijacking

Phishing, fraud, and software exploits are highly prevalent today, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data. Attackers may be able to use the cloud application to launch other attacks. Organizations must prohibit sharing of account credentials between users and services and must enable multifactor authentication schemes where available. Accounts, must be monitored so that every transaction should be traced to a human

owner. The key is to protect account credentials from being stolen.

### 3.1.6 Permanent data loss

Hackers have in the past have permanently deleted data from cloud to cause harm businesses and cloud data centers are as vulnerable to natural disasters as any facility. Cloud providers may recommend distributing applications and data across multiple zones for better protection. Adequate data backup measures and disaster recovery are very important. Daily data backup and off-site storage are very important with use of cloud environments. The burden of preventing data loss is not only of cloud service provider, but also of data provider.

## Chapter IV:

## 4.1 SECURITY CHALLENGES OF SERVICE MODEL:

### 4.1.1 Malicious attacks

Security threats can occur from both outside of and within organizations. According to the 2011 Cyber Security Watch Survey 21% of cyber-attacks were caused by insiders. 33% of the respondents thought the insider attacks were more costly and damaging to organizations.

### 4.1.2 Backup and Storage

The cloud vendor should ensure that regular backup of data is implemented that even ensure security with all measures. But the backup data is generally found in unencrypted form which can lead to misuse of the data by unauthorized people. Thus data backups lead to various security threats. More the server virtualization increases, an extremely difficult problem with backup and storage is created. Data de-duplication is one of the solutions to reduce backup and offline storage volumes.

### 4.1.3 Service hijacking

Service hijacking is means gaining illegal control on certain authorized services by unauthorized users. It can be through various techniques like phishing, exploitation of software and fraud. This is as one of the threats. Account Hijacking has been pointed as one of the most serious threats [13]. The chances of hijacking account are incredibly high as no native

### 4.1.4 VM Hopping

The attacker can check the victim/users VM's resource procedure, alter the configurations and can even delete stored data which may be sensitive, therefore, putting it in danger the VM's confidentiality, integrity, and availability. A requirement for this type of attack is that the two VMs must be operating on the same host, and the attacker must be able to recognize the victim VM's IP address. Though PaaS and IaaS users have partial authority, an attacker may get hold of or decide the IP address using benchmark customer capabilities by using various tricks and combinational inputs to fetch user's IP. Thus it can be said that VM hopping is a rational threat in cloud computing.

## Chapter V:

## REAL LIFE EXAMPLES:

### 5.1 Home Depot

More than 56 million credit or debit cards and approximately 53 million emails compromised, this damage was even more severe from Home Depot's attack. A malware accessed a POS system that gave hackers entry into to Home Depot's systems over nearly a six month period. Hackers used a third-party vendor's user name and password to gain access Home Depot's network.The stolen information about credentials provided direct access to the organizations point-of-sale devices, hackers then acquired greater rights that allowed them to navigate portions of Home Depot's network and to deploy custom-built malware on its self-checkout systems in the US and Canada. These files did not contain passwords or other sensitive information, but phishing scams are a real danger.

**Chapter VI:**

## Conclusion

Cloud Computing is a new concept that presents quite a number of benefits for its users. But it also raises some security problems which may affect its usage. Understanding about the vulnerabilities existing in Cloud Computing will help organizations to make the shift towards using the Cloud. Since Cloud Computing leverages many technologies and it also inherits their security issues. Traditional web applications, virtualizations have been looked over but some of the solutions offered by cloud are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which differ depending on the model. As described in this paper, storage and networks are the biggest security concerns in Cloud Computing. Virtualization that allows multiple users to share a physical server is a major concerns for cloud users.. Virtual networks are target for some attacks. We have focused on this distinction, where we consider important to understand these issues. Another core element of cloud computing is multilatency.

**Chapter VII:**

## REFERENCES

[1]. Mohamed Magdy Mosbah, "Current Services in Cloud Computing: A Survey ," International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.3,No.5,October 2013

[2]. Armbrust, M. et. al., (2009), "Above the clouds: A Berkeley view of Cloud Computing", UC Berkeley EECS, Feb 2010.

[3]. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[4]. B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009

[5]. National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011.

[6]. D. Jamil and H. Zaki, "Security Issues in Cloud Computing and Countermeasures," International

[7]. Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011 http://www.infoworld.com/article/3041078

[8]. Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, and Security, CRC Press; 2009.

[9]. Garfinkel T, Rosenblum M: When virtual is harder than real: Security challenges in virtual machine based computing environments. In Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. CA, USA: USENIX Association Berkeley; 2005:227–229.

[10]. Morsy MA, Grundy J, Müller I: An analysis of the Cloud Computing Security problem. In Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC; 2010.

[11]. Farzad Sabahi, "Cloud Computing Security Threats and Responses", 978-1-61284-486-2, IEEE, 2011, pp: 245 – 249.

[12]. Intel IT Center, "Preparing your Virtualized Data Center for the Cloud", pp: 1 – 20.