e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

REASEARCH IN CLOUD COMPUTING SECURITY

Mr. Ravend Kumar Upadhyay*1

*1Department Of Information Technology S.I.W.S College, Wadala, Mumbai – 400031, India.

ABSTRACT

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.

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, cloudcomputing 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 andcloud 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).

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. [2]. 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 [3].

CLOUD COMPUTING MODELS

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

Cloud computing deployment models

A.) 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 areoffered for various services given to the public cloudsubscribers 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 iseconomical. 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.

B.) 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 [4].

C.) 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. Hybridclouds 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 resourcesare 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.

D.) Community Cloud

It is a type of cloud hosting in which the setup is mutually shared between a lot of organizations which belong to a particular community like banks and trading firms. It is a multi-tenant setup that is shared among many organizations that belong to a group which has similar computing apprehensions. Theses community members usually share similar performance and security concerns. The main intention of the communities is to achieve business related objectives. Community cloud can be managed internally or can be managed by third party providers and hosted externally or internally. The cost is shared by specific organizations within the community, therefore, community cloud has cost saving capacity. Organizations have realized that cloud hosting has a lot of potential. To be the best one must select the right type of cloud hosting Therefore, one need to know the business and analyze his/her demands. Once the appropriate type of cloud hosting is selected, one can achievebusiness related goals easily.

CLOUD SERVICE MODELS:

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 [5]. 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.

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.

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.

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 [6]. 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.

Threats in cloud computing

A.) Compromised credentials and brokenauthentication

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 .

B.) 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.

C.) Hacked interfaces and APIs

Today every cloud service and application now offers APIs. IT teams use these interfaces and APIs to manage

and interact with cloud services, including those that offer cloud provisioning, management and monitoring. The security and availability of cloud services depend on the security of the API. Risk is increased with third parties who rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials. APIs and Weak interfaces may expose organizations to security related issues such as confidentiality, accountability, availability APIs and interfaces are the very much exposed part of the system because they can be accessed from open Internet .

D.) Exploited system vulnerabilities

Vulnerabilities in system, exploitable bugs in programs have become a bigger problem with the advent of multitenancy in cloud computing. Organizations share memory, databases and resources in close proximity to one another, creating new attack surfaces. The costs of mitigating system vulnerabilities are relatively small compared to other IT expenditures. The expense of putting IT processes in place to find and repair vulnerabilities is small when compared to the potential damage.

E.) Account hijacking

Phishing, fraud, and software exploits are highly prevalent today, and cloud services add a newdimension 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.

F.) 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. customer may encrypt data before uploading it on the cloud, then that customer has to be careful to protect the encryption key. If the key is lost then the data will also be lost. Compliance policies many a times specify how long organizations must retain records of audit and other documents. Losing such sensitive data may have serious consequences.

SECURITY CHALLENGES OF SERVICEMODEL

A.) 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. Generally, inside attacks were unauthorized access to and use ofcorporate information (63 %), and theft of intellectual property (32%). Malicious users can gainaccess to certain sensitive data and thus leading to data breaches. Farad Sabah [11] has shown malicious attacks by the unauthorized users on the victim's IP address and physical server. The malicious agenda can vary from data theft to revenge. In a cloud scenario, an insider can destroy whole infrastructures or manipulate or steal data.Systems that depend solely on the cloud service provider for security are at greatest risk.

B.) Backup and Storage

The cloud vendor should ensure that regularbackup 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 [12]. Data de-duplication is one of the solutions to reduce backup and offline storage volumes.

C.) Service hijacking

Service hijacking is means gaining illegal control on certain authorized services byunauthorized 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 hijackingaccount are incredibly high as no native

D.) VM Hopping

The attacker can check the victim/users VM's resource procedure, alter the configurationsand 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 byusing 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.

Security challenges of deployment model

Platform-as-a-service (PaaS) security issues

PaaS allows deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers [14]. PaaS depends on a secure and reliable network. PaaS application security constitutes two software layers: Security of the PaaS platform itself and Security of customer applications deployed on a PaaS platform.

Third-party relationships

PaaS along with traditional programminglanguages also offers third-party web services components such as mashups [15]. Mashups can combine more than one source element into a single integrated unit. Therefore PaaS models have securityissues which are related to mashups [16]. PaaS users are dependent on both the security of web- hosted development tools and third-party services.

Development Life Cycle

From the point of view of the application development, developers may face the complexity ofbuilding secure applications that may be hosted inthe cloud. The speed at which applications change inthe cloud will affect both the security and System Development Life Cycle (SDLC) [17]. Software Developers have to keep in mind that PaaS applications must be upgraded frequently hence they have to make sure that their application development processes are flexible enough to keep up with changes. However, software developers should understand that any change in PaaS components can compromise the security of the applications. Other than secure development techniques, developers need to be educated and informed about data legal issues as well, so that data is not stored ininappropriate locations. Data may be stored in different places with different legal regimes that can include its privacy and security.

Underlying infrastructure security

In PaaS, software developers do not normally have access to the underlying layers, so providers are therefore responsible for securing the underlying infrastructure and the applicationsservices. Even if developers are in control of the security, they do not have the assurance that thedevelopment environment tools provided by a PaaS provider are secure.

Cloning and Resource Pooling

Cloning means with replicating orduplicating the data.. Cloning can lead to data leakage problems which reveal the machine's authenticity. While Wayne A. Pauley [18] describes resource pooling as a service provided to the usersby the provider to use various resources and sharethe same according to their application demand. Resource Pooling means unauthorized access due to sharing through the same network. Studies on Virtual and Cloud Computing by researchers state that a Virtual Machine can quite easily be provisioned, they can also be inversed to previous cases, paused and easily restarted and migrated between two servers, leading to non-auditable security threats

Unencrypted Data

Data encryption is a process that helps to solve various external and malicious threats Unencrypted data is very vulnerable for susceptible data, as it does not provide any security mechanism. Unencrypted data can very easily be accessed by unauthorized users. Unencrypted data risks the user data which leads to cloud server to escape various data information to unauthorized users [19]. For example, the famous file sharing service Drop box was accused for using a single encryption key for all user data the company stored. These unencrypted, insecure data encourage the malicious users to misuse the data one or the other way.

Authentication and Identity Management

With the use of cloud, a user is facilitated toaccess private data and makes it available to various services across the network. Identity management helps in authenticating the users through their credentials. A key issue, concerned with Identity Management (IDM), is its disadvantage of interoperability resulting from different identitytokens and identity negotiation protocols as well as the architectural pattern [20].

Network Issues

Cloud computing relies on internet and remote computers so that it can maintain data for running various applications. This network is used to upload all information. H.B. Tabakki [21] has stated security issues with network on cloud as a prime focus. It provides virtual resources, high bandwidth and software to the consumers on demand. In reality, the network structure of this cloud is vulnerable to various attacks and security issues like cloud malware injection attack, browser security issues, flooding attacks, locks-in, incomplete data deletion, data protection and XML signature elementwrapping.

XML Signature Element Wrapping

It is a very renowned web service attack. This protects identity value and host name from illegal party but cannot protect the position in the documents [22]. The attacker targets the host computer by sending SOAP messages and putting scrambled data which the user of the host computer will not understand. The XML Signature wrapping attack changes the content of the signed part of a message and does not tamper the signature. Thiswould not let the user to understand.

Browser Security

Client uses browser to send the information on network. These browsers use SSL technology to encrypt user's identity and credentials. But hackers from the intermediary host may obtain these credentials by using sniffing packages installed on the intermediary host. One should have a single identity but this credential must allow different levels of assurance which can be achieved by obtaining approvals digitally.

Flooding Attacks

In this type of attack the invader sends largenumber of requests for resources on the cloud rapidly so that the cloud gets flooded with the large number of requests. As per the study carried out by IBM [23] cloud has a property to expand on the basis of amount of request. It will expand in so that it fulfills the requests of invader making the resources inaccessible for the normal users.

REAL LIFE EXAMPLES

A.) Target

Target security breach leakedapproximately 70 million customer's credit card information during 2013. Similar to iCloud, Target's network breach revealed that it had many holes in the company's security strategy. The Target hackwas the result of access to network via an HVAC contractor monitoring store climate systems, so oncethe Target system was breached, the hackers simply uploaded a grabber program to mirror payment data to Target server which was unused. Hackers accessed the payment stream -- plump with holiday shopper's information -- for two months. Target faced losses of $400 million -- plus a great deal of customer trust. It cost CEO his jobs. Hackers had gained access to Target's network for close two weeks in 2013. Target has now taken measures to plug any security holes, but the intrusion could have been avoided. An intrusion detection package had warned of this attack on multiple occasions, but those warnings were ignored.

B.) 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-checkoutsystems in the US and Canada. These files did not contain passwords or other sensitive information, butphishing scams are a real danger.

II. 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 multitenancy.

III. REFERENCES

[1] 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.

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

[3] National Institute of Standards and Technology, NIST Definition of CloudComputing, Sept 2011.

[4] D. Jamil and H. Zaki, "Security Issues in Cloud Computing and Countermeasures," International Journal of Engineering Science andTechnology, Vol. 3 No. 4, pp. 2672-2676, April 2011.

[5] http://www.infoworld.com/article/3041078

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

[7] 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.

[8] 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.

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

[10] Intel IT Center, "Preparing your VirtualizedData Center for the Cloud".