Journal of Engineering Sciences
Vol 11, Issue 6,June/2020
ISSN NO:0377-9254

An Analysis of Security Issues In Cloud

J.Samatha
Assistant Professor
samathajuluri@gmail.com

K.Bhagya Laxmi
Assistant Professor
bhagyareddy20380@gmail.com

***Abstract*- The computational world is becoming very large and complex. Cloud computing has emerged as a popular computing model to support processing large volumetric data using clusters of commodity computers. Cloud Computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Cloud computing may be defined as management and provision of resources, software, applications and information as services over the cloud (internet) on demand. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. This paper firstly lists the parameters that affect the security of the cloud and then we discuss security issues in cloud including storage security, data security and network security.**

Keywords— **Cloud computing, Threats, Security.**

I. INTRODUCTION

Cloud computing is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts. In simple words, Cloud Computing[1], is the combination of a technology, platform that provides hosting and storage service on the Internet . Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels .

Cloud computing is the collection of virtualized and scalable resources [2], capable of hosting application and providing required services to the users with the "pay only for use" strategy where the users pay only for the number of service units they consume. A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way. [7]

II. WHAT IS CLOUD COMPUTING

The cloud refers to the data center hardware and software that supports client's needs, often in the form of data stores and remotely hosted applications. These infrastructures enable companies to cut costs by eliminating the need for physical hardware, allowing companies to outsource data and computations on demand. Developers with innovative ideas for Internet services no longer need large capital outlays in hardware to deploy their services; this paradigm shift is transforming the IT industry. The operation of large scale, commodity computer data centres was the key enabler of cloud computing, as these data centres take advantage of economies of scale, allowing for decreases in the cost of electricity, bandwidth, operations, and hardware.

Cloud computing is a style of computing [6] in which dynamically scalable and often virtualized resources are provided as a service. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Furthermore, cloud computing employs a model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services)[8] that can be rapidly provisioned and released with minimal management effort or service provider interaction.

From a hardware point of view [3], three aspects are new in Cloud Computing:

1. The illusion of infinite computing resources available on demand, thereby eliminating the need for Cloud Computing users to plan far ahead for provisioning.
2. The elimination of an up-front commitment by Cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs and
3. The ability to pay for use of computing resources on a short-term basis as needed (e.g. processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful.

III. TAXONOMY OF CLOUD COMPUTING

Cloud computing is a general term for anything that involves delivering hosted services over the Internet[6]. These services are broadly divided into four categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) , Software-as-a-Service (SaaS), Hardware-as-a-Service (HaaS), Network-as-a-Service (NaaS).

A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider.) A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services. Hybrid cloud [1] environment consists of multiple internal and/or external providers.

Fig1 shows the layered architecture of cloud computing[1].

Software -as-a- Service (SaaS)
Platform -as-a- Service (PaaS)
Infrastructure -as-a- Service (IaaS)
Hardware -as-a- Service (HaaS)
Network -as-a- Service (NaaS)

Fig. 1 cloud layered architecture

Infrastructure-as-a-Service like Amazon Web Services provides virtual server instanceAPI) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed, it's sometimes referred to as utility computing.

Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer. Force.com, (an outgrowth of Salesforce.com) and GoogleApps are examples of PaaS. Developers need to know that currently, there are not standards for interoperability or data portability in the cloud. Some providers will not allow software created by their customers to be moved off the provider's platform.

In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS is a very broad market. Services can be anything from Web-based email to inventory control and database processing. Because the service provider hosts both the application and the data, the end user is free to use the service from anywhere.

Hardware-as-a-service is the idea of buying [12] or even an entire data center as a pay-as-you-go subscription service that scales up or down to meet the needs. But as a result of rapid advances in hardware virtualization, IT automation and usage metering and pricing, Hardware –as-a-service may at last be ready for prime time. This model is advantageous to the enterprise users, since they do not need to invest in building and managing data centers[15].

Network-as-a-service: Running a business demands fast and reliable connectivity and this typically takes the form of investing in network hardware and staff for round-the-clock network management. With NaaS (Network as a Service) this is all in the past. All you require now is a computer and an Internet connection to connect to your service provider network portal. NaaS is a cloud model, which provides businesses with network services over the Internet on pay-per-use or subscription consumption models. Network, the backbone of any company's IT structure, is now available as a service. The biggest advantage of NaaS is the complete control and flexibility that businesses can gain. Network administrators can exert total control on the allocation and provisioning of the bandwidth and as the network now exists in a virtual world, there is endless flexibility for network capacity and scalability. This flexibility also extends to the location of the business and of course, pricing models. Shifting network services to the cloud saves the cost of investing in and running network infrastructure. This is guaranteed to result in immense cost savings for business that are running applications with thousands of users. For companies with seasonal or sudden burst in workload NaaS allows instant ramp up and down of network capacity with just a few clicks. With Network as a Service, businesses can eliminate all the hassle of managing and maintaining the network. The

infrastructure and its complexities are invisible to the client; it is all taken care of by the service provider.

IV. Advantages of Cloud Computing [4]:

The following are some of the major advantages of cloud computing:

- Virtualization: Virtualization is defined as decoupling and separation [2] of the business service from the infrastructure needed to run it.
- Flexibility to choose vendor.
- Elasticity: Elastic nature [2] of the infrastructure allows to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis.
- Cost Reduction: Reduced costs due to operational efficiencies, and more rapid deployment of new business services.

V. Parameters affecting cloud security

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems[9], virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

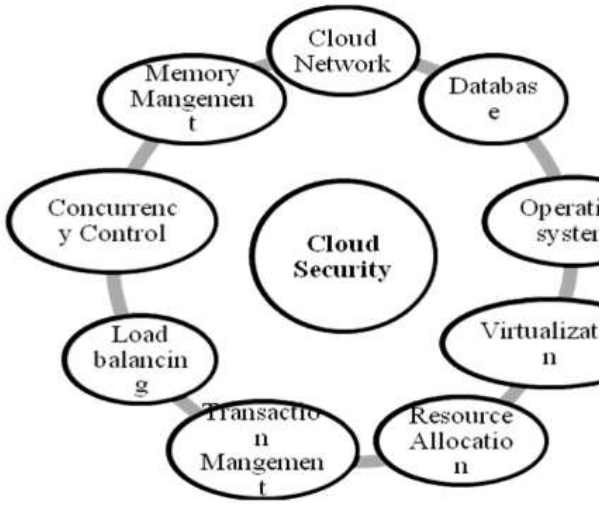

Fig 2: Parameter that affects cloud security

Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns[14]. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

VI. Security Issues

The security of corporate data in the cloud is difficult, as they provide different services like Network as a service (NaaS), Platform as a service (PaaS), Software as a service (SaaS), Infrastructure as a service (IaaS). Each service has their own security issues.

Data Security: Data Security refers as a confidentiality, integrity and availability. These are the major issues for cloud vendors. Confidentiality is defined as a privacy of data. Confidentiality are designed to prevent the sensitive information from unauthorized or wrong people. In this stores the encryption key data from enterprise C, stored at encrypted format in enterprise D. that data must be secure from the employees of enterprise D. Integrity is defined as the correctness of data, there is no common policies exist for approved data exchanges. Availability is defined as data is available on time.

Regulatory Compliance: Customers are eventually accountable when the security and completeness of their own data is taken by a service provider[13]. Traditional service providers more prone to outsource surveys and security certification. Cloud computing providers reject to endure the scrutiny as signaling so these customers can only make usage of paltry operations .

Data Locations: When users use, they probably won't know exactly where their data will hosted and which location it will stored in. In fact, they might not even know what country it will be stored in. Service providers need to be asked whether they will accomplish to storing and alter data in particular arbitration, and on the basis of their customers will they make a fair accomplishment to follow local privacy requirement[9].

Privileged user access: Outside the resource data that is processed contains an indigenous risk, as deploy services, avoid the mortal, consistent and human resource manage IT shops works on the house programs.

Trust Issue: Trust is also a major issue in cloud computing. Trust can be in between human to machine, machine to human, human to human, machine to human. Trust is revolving around assurance and confidence. In cloud computing, user stores their data on cloud storage because of trust on cloud. For example people use Gmail server, Yahoo server because they trust on provider.

Data Recovery: It is defined as the process of restoring data that has been lost, corrupted or accident.

Cloning and Resource Pooling: Cloning deals with replicating or duplicating the data. Cloning leads to data leakage problems revealing the machine's authenticity. While resource pooling as a service provided to the users by the provider to use various resources and share the same according to their application demand. Resource Pooling relates to the unauthorized access due to sharing through the same network.

Mobility of Data and Data residuals: For the best use of resources, data often is moved to cloud infrastructure. As a result the enterprise would be devoid of the location where data is put on the cloud. This is true with public cloud. With this data movement, the residuals of data is left behind which may be accessed by unauthorized users. Data-remnant causes very less security threats in private cloud but severe security issues may evolve in public cloud donations. This again may lead to data security threats like data leakage, data remnants and inconsistent data,

Elastic Perimeter: A cloud infrastructure, particularly comprising of private cloud, creates an elastic perimeter. Various departments and users throughout the organization allow sharing of different resources to increase facility of access but unfortunately lead to data breach problem. In private clouds, the resources are centralized and distributed as per demand[5]. The resource treatment transfers resources based on the requirements of the users thus leading to problems of data loss, where any user may try to access secure data with ease. Moreover, The elasticity of various cloud based resources would lead to store replicated data on untrusted hosts and this would then lead to enormous risks to data privacy.

Shared Multi-tenant Environment: Multitenancy is one of the very vital attribute of cloud computing, which allows multiple users to run their distinct applications concurrently on the same physical infrastructure hiding user data from each other. But the shared multi-tenant character of public cloud adds security risks such as illegal access of data by other renter using the same hardware. A multi-tenant environment might also depict some resource contention issues when any tenant consumes some unequal amount of resources.

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

Authentication and Identity Management: With the help of cloud, a user is facilitated to access its private data[5] and make 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 the disadvantage of interoperability resulting from different identity tokens and identity negotiation protocols as well as the architectural pattern. IDM leads to a problem of intrusion by unauthorized users. In order to serve authentication, apart from providing a password, a multi-factor authentication using smart card and fingerprint must be implemented for attaining higher level of security.

Data Leakage and consequent problems: Data deletion or alteration without backup leads to certain drastic data-related problems like security, integrity, locality, segregation and breaches[10]. This would lead to sensitive data being accessed by the unauthorized users. Cloud platforms should provide new services in order to collect context information and to perform analysis and manage data privacy so as to support applications requesting the information. One solution to this data leakage problem, is deduplication with allowing a limitation on number of user uploads per time window. The term deduplication means storing only a single copy of redundant data

and providing just a link to this copy rather than storing actual copies of this data.

Malicious Attacks: The threat of malicious attackers is augmented for customers of cloud services by the use of various IT services which lacks the lucidity between the procedure and process relating to service providers. Malicious users may gain access to certain confidential data and thus leading to data breaches. An access control mechanism tool can be thought of to control unauthorized user in accessing secured data Infrastructure as a Service as one of the models that exposes challenges with using virtualization as a frontier security protection to defend against malicious cloud users.

Backup and Storage: The cloud vendor must ensure that regular backup of data is implemented that even ensure security with all measures[12]. But this backup data is generally found in unencrypted form leading to misuse of the data by unauthorized parties. Thus data backups lead to various security threats. As the server virtualization increases, a very difficult problem with backup and storage is created. Data de-duplication is listed as one of the solution to reduce backup and offline storage volumes. De-duplication in cloud storage is carried out with the misuse of data backup.

Shared Technological issues: IaaS vendors transport their services in a scalable way by contributing infrastructure. But this structure does not offer strong isolation properties for a multi-tenant architecture. Hence in order to address this gap, a virtualization hypervisor intercede the access between guest operating systems and the physical compute resources.In spite of several advantages, these hypervisors have exhibited flaws that have permitted guest operating systems to expand inappropriate levels of control or authority on the underlying platform. This certainly led to security issues on the cloud.

Service Hijacking: Service hijacking is associated with gaining an illegal control on certain authorized services by various unauthorized users[10]. It accounts for various techniques like phishing, exploitation of software and fraud. This is considered as one of the top most threats. Account hijacking has been pointed as one of the severe threats. The chances of hijacking ones account increases considerably as no native API's are used for registering various cloud services.

VM Hopping: an attacker on one VM gains rights to use another victim VM. The attacker can check the victim VM's resource procedure, alter its configurations and can even delete stored data, thus, putting it in danger the VM's confidentiality, integrity, and availability[5]. A requirement for this attack is that the two VMs must be operating on the same host, and the attacker must recognize the victim VM's IP address. Although PaaS and IaaS users have partial authority, An attacker can get hold of or decide the IP address using benchmark customer capabilities on the basis of various tricks and combinational inputs to fetch user's IP. Thus it can be inferred that VM hopping is a rational threat in cloud computing. Additionally, multi-tenancy makes the impact of a VM hopping attack larger than in a conventional IT environment. Because quite a few VMs can run at the same time and on the same host there is a possibility of all of them becoming a victim VMs. VM hopping is thus a critical vulnerability for IaaS and PaaS infrastructures.

VM Mobility: The contents of VM virtual disks are saved as files such that VMs can be copied from one host to another host over the system or via moveable storage devices with no physically pilfering a hard drive[11]. VM mobility might offer quick use but could show the way to security problems likewise, the rapid spread of susceptible configurations that an attacker could make use of to endanger the security of a novel host. Several types of attacks might take advantage of weaknesses in VM mobility which includes man in-the-middle attacks. The severity of the attacks ranges from leaking perceptive information, to completely compromising the guest OS. Moreover, VM mobility augments the complication of security management because it offers augmented flexibility. In the IaaS model, a provider presents resources and underlying hardware as a service and a user can produce his or her possessed computing platform by importing a personalized VM representation into the infrastructure service. The huge scale of IaaS makes VM mobility's force on confidentiality and integrity in the cloud possibly outsized than in a conventional IT environment. A PaaS provider offers a variety of pre-configured computing platform and solution stacks to the service users. The users take advantage of the libraries and APIs to build up their individual applications on a permanent computing platform by importing their VM images. Although PaaS considers virtualization as a key implementation technology, it does not hold up VM mobility, therefore this service

model is not having the same security challenges as a traditional IT environment. While the confidentiality, integrity and availability of PaaS, SaaS and DaaS (Database-as-a-Service) are still open to the elements, the threats rose from IaaS.

VM Denial of Service: Virtualization lets numerous VMs split physical resources like CPU, network bandwidth and memory or disk[12]. A Denial-of-Service or DoS attack in virtualization takes place when one VM occupies all the obtainable physical resources such that the hypervisor cannot hold up more VMs and accessibility is endangered. The most excellent move towards preventing a DoS attack is to bound resource allocation using correct configurations. In cloud computing, DoS attacks could still happen, but having service providers place sufficient configurations to put a ceiling on the resources owed to the VMs decreases their probability. Additionally, it is advisable to have the Service Level Agreement (SLA). This legally identifies responsibilities of the service provider and the user.

Browser Security: Every client uses browser to send the information on network. The browser uses SSL technology to encrypt user's identity and credentials. But hackers from the intermediary host may acquire these credentials by the use of sniffing packages installed on the intermediary host. In order to overcome this, one should have a single identity but this credential must allow various levels of assurance which can be achieved by obtaining approvals digitally.

SQL Injection Attack: These attacks are malicious act on the cloud computing in which a spiteful code is inserted into a model SQL code. This allows the invader to gain unauthorized access to a database and eventually to other confidential information. Further, SQL injection attacks uses the special characters to return the data for example in SQL scripting the query usually ends up with where clause which again may be modified by adding more rows and information in it. The information entered by the hacker is misread by the website as that of the user's data and this will then allow the hacker to access the SQL server leading the invader to easily access and modify the functioning of a website.

Flooding Attacks: In this attack the invader sends the request for resources on the cloud rapidly so that the cloud gets flooded with the ample requests[5]. As per the study carried out by IBM, cloud has a property to expand on the basis of large amount of request. It will expand in order to fulfill the requests of invader making the resources inaccessible for the normal users.

Incomplete Data Deletion: Incomplete data deletion is treated as hazardous one in cloud computing. When data is deleted, it does not remove the replicated data placed on a dedicated backup server[11]. The operating system of that server will not delete data unless it is specifically commanded by network service provider. Precise data deletion is majorly impossible because copies of data are saved in replica but are not available for usage.

Locks in: Locks in is a small tender in the manner of tools, standard data format or procedures, services edge that could embark on data, application and service portability, not leading to facilitate the customer in transferring from one cloud provider to another or transferring the services back to home IT location.

VI. CONCLUSION

Cloud computing is latest technology that is being widely used all over the world. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. In this paper, we have discussed the parameters that effect the cloud security, and also discussed various security issues encountered in cloud services.

REFERENCES

[1] Bhaskar Prasad Rimal,Eunmi choi,Ian Lumb A Taxonomy and Survey of Cloud Computing Syatems ,2009 IEEE.

[2] Shilpashree Srinivasamurthy, David Q. Liu, Survey on Cloud Computing Security

[3] Michael Armbrust, Armando Fox, Rean Griffith, Above The Clouds :A Berkeley View Of Cloud Computing,2009

[4] Amit Goyal, Sara Dadizadesh,A Survey on Cloud Computing Technical Report for CS 508, December 2009.

[5] Ms. Disha H. Parekh Dr. R. Sridaran An Analysis of Security Challenges in Cloud Computing (IJACSA) Vol. 4, No.1, 2013 .

[7] Manpreet Kaur, Hardeep Singh "A Review Of Cloud Computing Security Issues" International Journal of Advances in Engineering & Technology, June, 2015. 397 Vol. 8, Issue 3, pp. 397-403

[8] Feng-Tse Lin, Teng-San Shih, "Cloud Computing: The Emerging Computing Technology," ICIC Express Letters Part B: Applications (ISSN: 2185-2766), v1, September 2010, pp. 33-38

[9] Prince Jain "Security Issues and their Solution in Cloud Computing " International Journal of Computing & Business Research 2012

[10] Monjur Ahmed,Mohammad Ashraf Hossain" Cloud Computing And Security Issues In The Cloud " International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014

[11] Steve Hanna. A security analysis of Cloud Computing, Cloud Computing Journal. DOI http://cloudcomputing.sys-con.com/node/1203943

[12] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy, An Enterprise perspective of Risks and compliance, O'Reilly Media, Inc,2009.

[13] Discovering Identity: Cloud Computing: Identity and Access Management DOI = http://blogs.sun.com/identity/entry/cloud_computing_identity_and_access

[14] Siegele,L, Let It Rise: A Special Report on Corporate IT. The Economist (October 2008).

[6] Open Security Architecture http://www.opensecurityarchitecture.org/

[15] Vogels, W. A Head in the Clouds—The Power of Infrastructure as a Service. In First workshop on Cloud Computing and in Applications (CCA '08) (October 2008).

AUTHOR'S BIBLIOGRAPHY

J.Samatha Asst.Professor,CSE Dept in MatrusriEngineering College,Hyderabad. She is M.Tech(CSE) from JNTU is in teaching field from past fourteen years. Her interested areas are Cloud Computing,Big Data,Deep learning.

K.Bhagya Laxmi Asst.Professor,CSE Dept in Matrusri Engineering College,Hyderabad. She is M.Tech(CSE) from JNTU is in teaching field from past fourteen years. Her interested areas are Cloud Computing ,Big Data, Data Mining.