ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Security Issues and Its Mechanisms in Cloud Computing: A Review

Monika Sharma, Amrita Ticku

M.Tech Student, Dept. of C.S., B.S.Anangpuria Institute of Technology, Faridabad, Haryana, India

Assistant Professor, Dept. of C.S., B.S.Anangpuria Institute of Technology, Dhauj, Faridabad, Haryana, India

ABSTRACT: Cloud computing is a platform that provides computing service via internet. It is dependent on demand and paid according to usage. It provides access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. It provide efficiency and many other advantages such as cost due to which it is used in many areas such as in education, banking etc.

Cloud computing is a promising technology to facilitate development of large-scale, on-demand, flexible computing infrastructures. Security is one of the main challenges that hinder the growth of cloud computing. Service providers strive to reduce the risks over the clouds and increase their reliability. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks.

This paper presents an overview of the cloud computing, the several security issues and a overview of mechanisms to deal with security issues.

KEYWORDS: Cloud Computing, Services, Security Issues, Mechanisms

I. INTRODUCTION

Cloud computing enables on-demand access to shared resources without physically acquiring them. NIST defined the term [3] “Cloud Computing” as an ubiquitous on-demand model for accessing common resources over a network.

The main idea of cloud computing is to deliver both software and hardware as services. There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis.

DOI: 10.15680/IJIRCCE.2016. 0406116

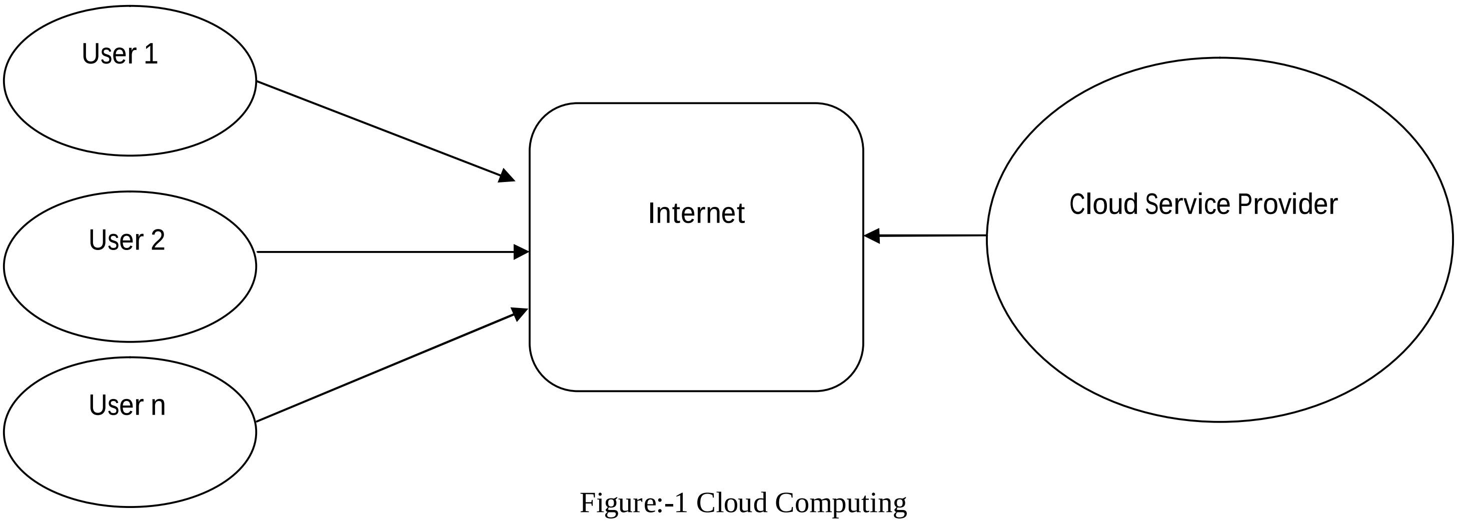

Figure:-1 Cloud Computing

Cloud computing is use of scalable computing resources over Internet on a pay-as-you-go basis [2]. It provides a cost-effective IT solution to business & scientific community. Economically the main attraction from Cloud computing is that customers only use what they need, and pay for what they actually use. Organizations neither need to purchase expensive hardware such as servers, storage, networking equipments etc. nor require manpower for development of complex IT solutions in-house.

Cloud computing offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Software-as-a-Service (SaaS): SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This application does not require that customer for installing and operating the application on their own computer and also eliminates the tremendous load of software maintenance. SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data center space, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. Examples of SaaS includes Best retail apps, Xangati,Google Apps[3].

Platform as a Service (PaaS): "PaaS provides a computing platform without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. There is no need for user to user manage the infrastructure (including network, servers, operating systems and storage), but user controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure[3].

Infrastructure as a Service (IaaS): Infrastructure as a service (IaaS) uses a virtualization technology in which hardware resources are shared for executing services. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. The service provider owns the equipment and is responsible for housing, running and maintaining it [1]. The client typically pays on a per-use basis. Examples of IaaS include Amazon Elastic Cloud Computing (EC2), Amazon S3, Go Grid.

II. CLOUD COMPUTING SECURITY ISSUES

These are the security issues which may occur during the usage of cloud computing.

i). Identification & authentication: **-** Identification and authentication is an important security issue in cloud computing. This methodology is states that there is no unauthorized to cloud services. Authorization is a vital information security requirement in Cloud computing to ensure referential integrity is maintain. Authorization is maintained by cloud service provider.

ii). Integrity: **-** Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

iii). Non-repudiation:- Non-repudiation in Cloud can be achieved by applying the conventional e-trade security conventions and token facilities to information transmission inside cloud provisions. for example, advanced marks, timestamps and assertion receipts administrations. .To overcomes these security issues in cloud computing many security encryption and decryption algorithms are proposed.

iv). Data Transmission: **-** It is important that data should be transmitted correctly. It goes to the correct user and it does not be modified in between. Encryption techniques and SSL/TLS protocols are used here. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication is used.

v). Virtual Machine Security: **-** Virtualization is one of the main components of a cloud. Virtual machines are dynamic i.e. it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time.

vi). Network Security:- Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc. A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. Sniffer attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network [4]. Reused IP address issues have been a big network security concern. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user [5].

vi). Data security: **-** To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP).Hypertext Transfer Protocol Secure (HTTPS) can be used for information security and data integrity and Secure Shell (SSH) are the most common adoption. In a traditional application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Cloud service providers such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host.[6].

vii). Data Privacy: - The data privacy is also one of the key concerns for Cloud computing. This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks [2].

viii). Data Location: - In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs [2]. In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be done using a central global transaction manger. Each application in the distributed system should be able to participate in the global transaction via a resource manager.

ix). Data Availability: - Data Availability is one of the prime concerns. When data is on remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable. The Cloud application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan needs to be considered.

x). Data Segregation: - Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data. Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

xi). Security Policy and Compliance: - Traditional service providers are subjected to external audits and security certifications. If a cloud service provider does not adhere to these security audits, then it leads to a obvious decrease in customer trust. Enterprises need to prove compliance with security standards, regardless of the location of the systems required to be in scope of regulation, be that on-premise physical servers, on-premise virtual machines or off-premise virtual machines running on cloud computing resources.

Nevertheless, using services over the cloud is accompanied with many doubts mostly about security issues. A survey conducted by IDC [9] shows the importance of the challenges for those considering cloud computing as an option. It is shown in Figure 2 that security is the most important concern.

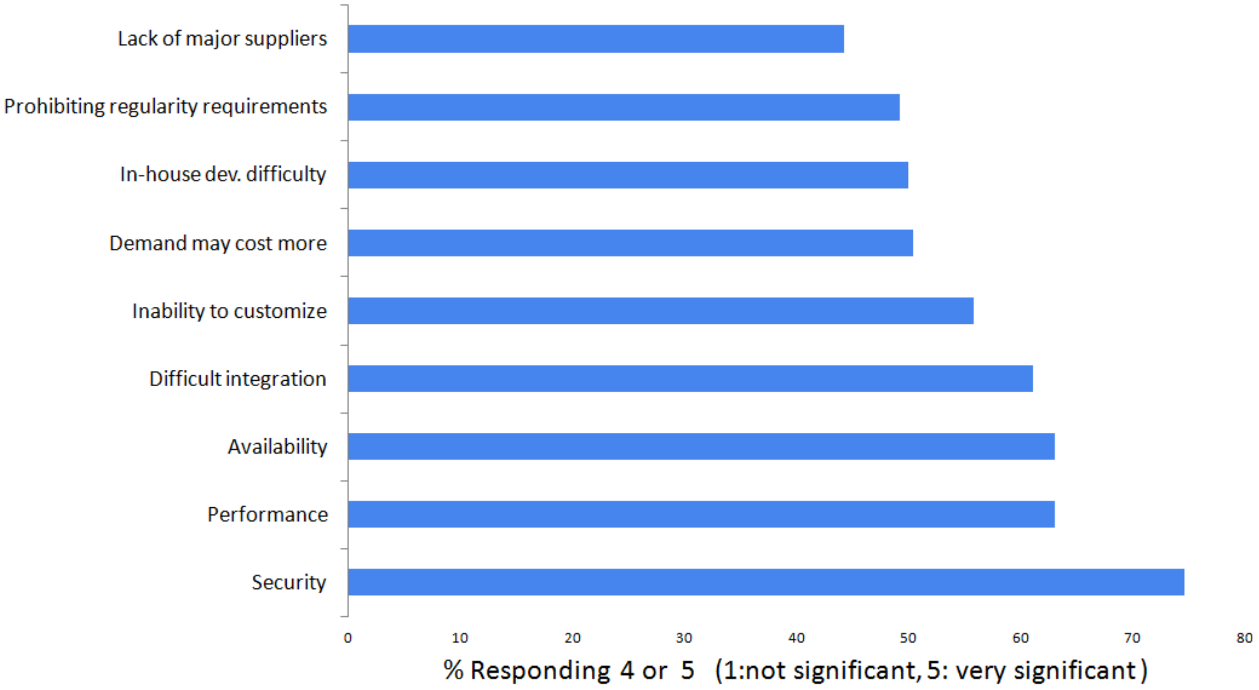

Figure 2. **Challenges in considering cloud computing (adapted from [9]).**

III. SECURITY MECHANISMS IN CLOUD COMPUTING

The mechanism that is used to deal with security of cloud computing are as follows:-

i). Encryption:-Data in readable format when transmitted over network is vulnerable to unauthorized person. Encryption is a mechanism which is used for confidentiality and integrity of data. It is used for encoding plaintext data in to protected and unreadable format. The main role of encryption is to take care of data secure from attackers. The process of getting back the original data from encrypted data is known as Decryption.There are two common forms of encryption known as symmetric encryption and asymmetric encryption are used to encrypt the data in cloud storage. Symmetric encryption uses the same key for both encryption and decryption, both of which are performed by authorized parties that use the one shared key. Also known as secret key cryptography, messages that are encrypted with a specific key can be decrypted by only that same key Note that symmetrical encryption does not have the characteristic of non- repudiation.

Asymmetric encryption relies on the use of two different keys, namely a private key and a public key. With asymmetric encryption (also referred to as public key cryptography), the private key is known only to its owner while the public key is commonly available. A document that was encrypted with a private key can only be correctly decrypted with the corresponding public key. Conversely, a document that was encrypted with a public key can be decrypted only using its private key counterpart. Asymmetric encryption is almost always computationally slower than symmetric encryption

Some of algorithms used are (a) RSA, a cryptographic algorithm whose encryption key is public and differs from the decryption key which is kept secret. (b) Data Encryption Standard (DES) and Simplifies Data Encryption Standard (S-DES), where DES used symmetric key for encryption and decryption. (c) Secure Socket Layer (SSL) 128 bit encryption, it is commonly-used protocol for managing the security of a message transmission on the Internet and it uses public and private key encryption system. (d) Mixed encryption algorithms. (e) RC5 which is a symmetric key block cipher and it consists of a number of modular additions and Exclusive OR (EXOR).

ii). Hashing:-The hashing mechanism is used when a one-way, non-reversible form of data protection is required. Once hashing has been applied to a message, it is locked and no key is provided for the message to be unlocked. A common application of this mechanism is the storage of passwords. Hashing technology can be used to derive a hashing code or message digest from a message, which is often of a fixed length and smaller than the original message. The message sender can then utilize the hashing mechanism to attach the message digest to the message. The recipient applies the same hash function to the message to verify that the produced message digest is identical to the one that accompanied the message. Any alteration to the original data results in an entirely different message digest and clearly indicates that tampering has occurred.

iii). Digital Signature:-The digital signature mechanism is a means of providing data authenticity and integrity through authentication and non-repudiation. A message is assigned a digital signature prior to transmission, which is then rendered invalid if the message experiences any subsequent, unauthorized modifications. A digital signature provides evidence that the message received is the same as the one created. There is no change in it. Both hashing and asymmetrical encryption are involved in the creation of a digital signature, which essentially exists as a message digest that was encrypted by a private key and appended to the original message. The recipient verifies the signature validity and uses the corresponding public key to decrypt the digital signature, which produces the message digest. Now a days digital signature are used with other method or protocols to make cloud storage more secure.

iv).Public Key Infrastructure (PKI):- A common approach for managing the issuance of asymmetric keys is based on the public key infrastructure (PKI) mechanism, which exists as a system of protocols, data formats, rules, and practices that enable large-scale systems to securely use public key cryptography. This system is used to associate public keys with their corresponding key owners (known as public key identification) while enabling the verification of key validity. PKIs rely on the use of digital certificates, which are digitally signed data structures that bind public keys to certificate owner identities, as well as to related information, such as validity periods. Digital certificates are usually digitally signed by a third-party certificate authority

v). Single Sign-On (SSO):-The authentication and authorization information for a cloud service consumer across multiple cloud services can be a challenge. The single sign-on (SSO)mechanism enables one cloud service consumer to be authenticated by a security broker, which establishes a security context that is persisted while the cloud service consumer accesses other cloud services or cloud-based IT resources. Otherwise, the cloud service consumer would need to re-authenticate itself with every subsequent request. The SSO mechanism essentially enables mutually authentication. For example a Kerberos protocol works on Single Sign On.

IV. RELATED WORK

1. Xiao S et.al [10] presents an algorithm to create dynamic credentials for cloud computing systems. The dynamic credential changes its value once a user changes its location or when he has exchanged a certain number of data packets.

2. Xiaopeng G et.al [11] proposed a security framework that customizes security policies for each virtual machine, and it provides continuous protection thorough virtual machine live migration. They implemented a prototype system based on Xen hypervisors using stateful firewall technologies and user space tools such as iptables, xm commands program and conntrack-tools. The authors conducted some experiments to evaluate their framework, and the results revealed that the security policies are in place throughout live migration.

3. Naehrig.M et.al [12] proposed Homomorphic encryption, the three basic operations for cloud data are transfer, store, and process. Encryption techniques can be used to secure data while it is being transferred in and out of the cloud or stored in the provider’s premises. Cloud providers have to decrypt cipher data in order to process it, which raises privacy concerns. In [12], they propose a method based on the application of fully homomorphic encryption to the security of clouds. Fully homomorphic encryption allows performing arbitrary computation on ciphertexts without being decrypted. Current homomorphic encryption schemes support limited number of homomorphic operations such as addition and multiplication. The authors in provided some real-world cloud applications where some basic homomorphic operations are needed. However, it requires a huge processing power which may impact on user response time and power consumption.

V.CONCLUSION AND FUTURE WORK

Cloud computing is recently a booming area and has been emerging as a commercial reality in the information technology domain. However the technology is still not fully developed. There are still some areas that are needed to be focused on. Security is one of them. This paper discuss about the cloud computing security issues and Challenges. Data security is major issue for Cloud Computing. There are several other security challenges including security aspects of network and virtualization. This paper analyzes cloud computing security issues and a mechanism how to deal with it. As the number of user increases, cloud becomes more vulnerable. Therefore, there is need to make them more secure. In future, more pragmatic security mechanisms are needed to make the cloud computing more secure.

REFERENCES

[1]. P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” Computer Security Division, IT Laboratory, National Institute of Standards and Technology, Gaithersburg, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800- 145.pdf

[2]. Rabi Prasad Padhy, Manas Ranjan Patra ,Suresh Chandra Satapathy,Cloud Computing: Security Issues and Research Challenges, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[3]. Osama Harfoushi1, Bader Alfawwaz2, Nazeeh A. Ghatasheh3, Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review, *Communications and Network*, 2014, 6, 15-21 Published Online February 2014 (http://www.scirp.org/journal/cn) http://dx.doi.org/10.4236/cn.2014.61003

[4]. Ohlman, B., Eriksson, A., Rembarz, R. (2009) What Networking of Information Can Do for Cloud Computing. The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Groningen, the Netherlands, June 29 - July 1, 2009

[5]. L.J. Zhang and Qun Zhou, “CCOA: Cloud Computing Open Architecture,” ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009.

[6]. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O’ Reilly Media, USA, 2009

[7]. Ronald L. Krutz, Russell Dean Vines “Cloud Security A Comprehensive Guide to Secure Cloud Computing”, Wiley Publishing, Inc.,2010

[8]. K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, “Intrusion detection techniques for Grid and Cloud Computing Environment,” IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010

[9]. F. Gens, “New IDC It Cloud Services Survey: Top Benefits and Challenges,” 2009. http://blogs.idc.com/ie/?p=730

[10]. Xiao S, Gong W (2010) Mobility Can help: protect user identity with dynamic credential. In: Eleventh International conference on Mobile data Management (MDM). IEEE Computer Society, Washington, DC, USA, pp 378–380)

[11]. Xiaopeng G, Sumei W, Xianqin C (2010) VNSS: “a Network Security sandbox for virtual Computing environment”. In: IEEE youth conference on information Computing and telecommunications (YC-ICT). IEEE Computer Society, Washington DC, USA, pp 395–398.

[12]. Naehrig M, Lauter K, Vaikuntanathan V (2011),Can homomorphic encryption be practical? In: Proceedings of the 3rd ACM workshop on Cloud Computing Security workshop. ACM New York, NY, USA, pp 113–124.

[13]. Rajarshi Roy, Security in Cloud Computing International Journal of Computer Application volume 96 –No-15,June 2014.