Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-3, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Cloud Security: A Big Challenge, Issues and Solutions

Anshul Garg[1] & Himanshi Babbar[2]
[1,2]Assistant Professor, Chandigarh Group of Colleges, Landran, Mohali

Abstract: *Cloud computing is a totally internet-based technology where customer data is stored and sustain in the data center of a cloud provider like Google, Amazon and Microsoft etc. The two key feature of this model are user-friendliness and cost- effectiveness. Restricted control over the data may invite various security issues which include data loss, Insecure Interfaces and APIs, resource Sharing, data availability and inside attacks, Account or Service Hijacking etc. There are various challenges also there for adopting cloud computing like well managed service level agreement (SLA), confidentiality, interoperability and reliability. This paper discuss the architecture of cloud security .It explores the layered wise cloud security issues and problems such as data, privacy, and infected application and also give their proposed solutions. It also explores various security attacks and how to handle that.*

Keyword: *Cloud Computing, Cloud service provider, Data Protection, User Authentication, Data Violation, Cloud security, Attacks in Cloud Computing.*

1. INTRODUCTION:

Cloud computing is a representation that enables suitable, Pay -as –you- use network access to a open pool of configurable computing assets such as networks, servers, storage, applications that can be quickly provisioned and released with negligible management effort or cloud service provider's communication. There are numerous reasons for organizations to move towards IT solutions that include cloud computing as they are just required to disburse for the resources on consumption basis. In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers [1]. Cloud computing opens many options for businesses, but with these opportunities there are number of security challenges that must be considered and addressed on priority basis before committing to a cloud computing strategy. Cloud security is the set of control-based technologies and policies that are designed to follow the rules and protect information, data applications and infrastructure associated with cloud computing use [2]. Cloud computing security challenges fall into three broad categories: Data Protection, User Authentication, Data violation

2. SECURITY ARCHITECTURE OF CLOUD COMPUTING:

Security architecture is the design that explains the necessary and prospective risks that can be occur in a certain environment [3]. It also explains where and when the security controls can be applied and how they are related to complete architecture [3]. By using these security controls we can guard any system's weakness and minimize the problem created by an attack. They can also protect system quality attribute like integrity, availability and confidentiality etc.

2.1 Cloud Computing Security Controls:-

There are many types of controls that we can use in Clouds but most of them come under the categories which we are explaining in the Table: 1

Sr.No	Control Type	Description
1	Deterrent controls	In this controls, The control informs the potential attackers that there can be problem for them if they proceed.
2	Detective controls	These controls detect the attack and react accordingly by sending the signal to preventive or corrective controls
3	Corrective controls	The control reduces the consequences of an event by limiting the damage.
4	Preventive controls	These controls give strength to the system by reducing the possibility of being attacked.

Fig. 1

2.2. **Layered Approach of Cloud Security Architecture**:-

Cloud computing security architecture is composed of four layers. This section of paper makes us understand about the functionality of each layer and some security issues that can occur in particular layer. It also tells what type of different skills required working with the different layers. Here is the high level cloud security architecture and the technological skills required to understand the aspects of cloud computing.

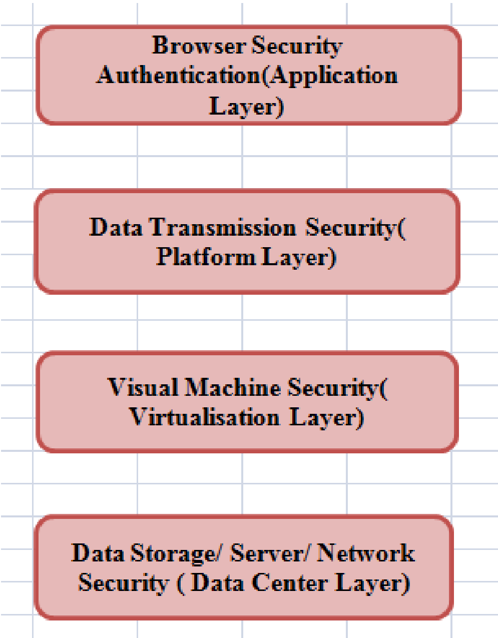

Fig. 2 High Level Security Architecture of Cloud Computing

2.2.1. Data Center Layer :-

The responsibility of data center or **hardware layer** is to manage the physical sources of cloud which include switches , cooling system, physical server, routers .This layer is usually used in Data centers where thousands of servers are arranged in racks and connected with each other through switches, routers and some other fabric[5]. So sometimes this layer is also called **Server Layer**. Security issues related with this layer are Server security, Network security, hardware configuration, traffic management, cooling and power resource management etc.

2.2.2. Virtualization Layer

The base of cloud technology is virtualization layer. This layer is also named as **Infrastructure layer**. This layer deploys a number of virtual machine on hardware and enables request of user in computing resources with the help of accessing the proper resources. "Virtual Machine" means sharing the resources of single computer into many other computers with in itself. To deal with this layer one must have the knowledge of connecting storage to virtualization host, distributing storage properly, networking etc. [5]. Some of the security issues in Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, Data leakage, Separation between Customers, Cloud legal and Regularity issues, Identity ,IP spooling, port scanning, Access management[7] .The examples of this layer are Flexi scale, Amazon EC2, and Go Grid etc.

2.2.3. Platform Layer:-

This layer contains operating systems and its application frameworks. The main motive of this layer is to minimize the load of deploying applications directly into VM containers [6]. Another name for this layer is **Service Provider layer**. The main components of platform layer are Scheduler & Dispatcher, Load Balancer, Advance Resource Reservation Monitor, and Policy Management and many more [5] .The desirable skills to handle this layer are to ensure that the system is accurately tuned for its role and maintaining optimal performance settings. Networking skills also required to ensure that cloud services are optimally deployed, delivered and maintained. Many types of security issues are like Identity, Infrastructure, Privacy, Data transmission, Auditing and Compliance, integrity and Binding Issues can be occur in this layer[7].Some examples of platform layer are, Google App Engine which is used to provide API support for implementing storage, business logic of web applications.[8]

2.2.4 The Application Layer

This is the most utilized layer of cloud computing, also called SaaS interface layer. In this layer application working is served via Internet. This layer is very close to end user. This layer has the responsibility of the management of the software and databases, including installation, updates and removal. This layer must have the knowledge of JavaScript, XML and Perl languages, as well as back-end infrastructure applications like Apache, Tomcat and SQL. [4]. This layer is further divided into three layers as shown in Fig-3

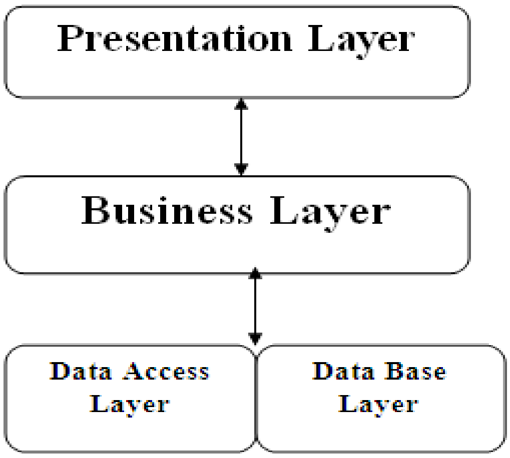

Fig. 3

1. The Presentation layer:- This layer explains the application user interactions,
2. The Business layer: -This layer explains the business logic.
3. The Data layer: - This layer is used for storage of application data..The data layer is subdivided into the Data Access Layer (DAL) which is used to encapsulates the data access functionality and data base layer (DBL) which is responsible for data persistence and data manipulation.[8]

3. LAYER BASED SECURITY THREATSAND SOLUTIONS:

In clouds, there are many issues as it encompasses a number of technologies like Database, Operating system, virtualization, Networks etc. So many security issues related to these technologies and systems also applied in cloud computing. [7]. In this section, we are discussing about various security issues that can occur on different layers and their possible solutions..

3.1 Data Center Layer

3.1.1. Security Threats:-

This layer deals with hardware. There are many security concerns at this layer. Some are

3.1.1.1 There are a no. of government rules and regulation about how to access, transact and store the data. Existing networking management tools don't allow logging of events and intrusion detection.[8]

3.1.1.2 Clocking problems in this layer can direct either to degrade performance or chronicle loss of connection.[9]

3.1.1.3 Increasing amount of data and devices can be a big security concern in physical layer

3.1.1.4 High maintenance cost has direct impact on operating expenses

3.1.1.5 True cloud computing require high bandwidth which can be a security issue on this layer.

3.1.1.6 As companies load up on Big Data and move to cloud so Data center cooling is becoming a hot topic in cloud environment

3.1.2. Security solutions:-

Some possible solutions in physical layer are as follows:-

3.1.2.1. Various encryption techniques are used before storing the data at virtual locations. In these techniques data is encrypted using keys and vendor must be prepared for security certifications and external audits. [8][10][11]

3.1.2.2. CSP should maximize the user control.

3.1.2.3. Organizations should run the applications and transfer their data on private cloud firstly then transmute it to public cloud.

3.2. Virtualization Layer

3.2.1 Security Threats:-

This layer is the fundamental layer. In this layer we are describing some important security threats.

3.2.1.1. One of the main problem of cloud computing is to build a new layer to maintain a main issue for Cloud computing is to build a new layer to maintain a negotiation phase between service consumers and provider to establish Service level agreement between them.

3.2.1.2 Virtual machine manager also called Hypervisor is a program to share single hardware resource among multiple operating systems. It controls the processor and hardware hosts. Two type of attacks can occur hypervisor first the attack on hypervisor via the host Operating System (OS) and secondly attacks on hypervisor via a guest OS. [11]

3.2.1.3. Port scanning which can be used by security technicians to audit the computers for vulnerabilities at the same times it can also be used by the hackers to target the victims.

3.2.1.4 Hackers can find out the IP address of trusted host and change the header of packet such that it assumes that packets are coming from host which can cause a big security issue.

3.2.1.5. Data leakage by offline images can also be a security threat in this layer.

3.2.2. Security Solutions:-
Some possible solutions in physical layer are as follows:-
3.2.2.1. Encryption techniques like Cipher text-ABE can be used for sending and receiving the data.
3.2.2.2. Unauthorized address can be control either by using access control list or by configuring the internet router.
3.2.2.3. High security web browser, Interruption Detection system or firewalls can be used to protect resources from attacks [8]

3.3. Platform Layer
3.3.1. Security Threats :-
In this layer security comprises two software layers: Firstly, the security of PaaS platform itself and secondly, the security of customer applications. In this section we are describing some security threats that can be occur on platform layer:-
3.3.1.1 In this layer, the software developers face very difficulty to secure the applications. The applications have to be upgraded by applying new versions or patches to keep them secure.
3.3.1.2. Sometimes particular vendors develop specific standards, protocols and tools for its particular cloud. This can make migration off a proprietary cloud platform expensive and complicated. [8][12]
3.3.1.3. In cloud environment, every framework has its own, service, cost and interface method. This unfolding nature of this layer puts everything at high risk.
3.3.2 Security Solutions:-
3.3.2.1. Signatures or Cryptographic can be used to detect the modifications if any.
3.3.2.2. PaaS providers are accountable for securing the platform software stack that includes the runtime engine that is used to run the applications.

3.4 Application Layer:-
3.4.1 Security Threats:-
This layer generally deals with end user via internet through web application, so all security issues that a web application faces can also be a security concern on this layer also. Some main application layer security issues are:-
3.4.1.1. Denial of service attack is the biggest security issue in application layer. In this hacker seeks to make the resources unavailable to its authorized user [14]. This is generally done by flooding the target machine with superfluous request in an attempt to overload the system such that system will not be able to fulfill some or all legitimate requests .[14]
3.4.1.2. Cloud computing environment provides numerous interfaces and APIs to communicate with the services provided to the organizations and third parties, at the same time This it also increases risk factor because sometimes organizations have to relinquish their credentials to third parties.
3.4.1. 3. Many other attacks like Dictionary attack, Buffer-overflow attack, Cross Site scripting, Service hijacking are also big security concerns on this layer.

3.4.2 Security Solutions
3.4.2.1. A runtime application self-protection tool can be very useful way for application security.
3.4.2.2. Two –factor authentication must be used for high level transactions.
3.4.2.3. Latest antivirus, spyware antivirus must be installed and update them without fail.
3.4.2.4. Cloud provider SLAs and security policies should ne understood clearly. [8]
3.4.2.5. Backups should be taken on regular interval.
3.4.2.6. Freeware should not be downloaded.

4. ATTACKS IN CLOUD COMPUTING

In today's world cloud computing is heading towards variety of services and interfaces that enable the number of vendors to run the services out on their physical machines at an hourly rate for the benefit of incentive.[17] So, therefore it has become more terrible and attackers follow it. The various attacks in cloud computing includes:

4.1 Denial of Service (DOS) attack: As cloud computing is perforated to the DOS attacks because as many users are indulged in the usage of many cloud services and other resources, DOS attack is becoming more damaging. In this attacker tries to attempt to intercept the legitimate the users from authorizing the information or resources of the network such as web service, website and many other computer systems. [18] The main drawbacks behind these situations are the network security that does not have the beneficial trackback methods to trace the attackers and try to detect the attackers effectively and efficiently.

Solution for DOS attack

For restricting the DOS attack, we will identify the traffic on the basis of the consent, so that we can block the traffic that is authenticated and permit the traffic that is not authenticated. [19] For this many firewalls are used to permit the traffic on the basis of protocols, ports and IP addresses. As all the traffic is coming the unauthorized IP addresses, a rule can be put down on the system of cloud computing that drop all the inaccessible or unauthorized incoming traffic. [17] As all the attached packets are forwarded to the "black hole" it would become more effective and efficient avoid the network infrastructure connectivity that is managed by the ISP systems.

4.2 Cloud Malware Injection Attack: In this type of attack, an attacker tries to inject the services of malicious into the cloud. [18] So in this attacker created their own malicious service implementation module (SaaS or PaaS) and try to add onto the system. If this succeeds, the system of cloud automatically redirects the valid user requests to the malicious implementation service [17] and the adversary's code is being accepted. The main motto of cloud malware injection attack is that the attacker uploads the controlled copy of the victim's service so that the malicious requests of service can be processed within the instance.

Solution for Cloud malware Injection attack

Usually when a customer wishes to open an account in the cloud, an image of the customer's virtual machine in the cloud will be provided by the provider. [17] In cloud system hypervisor is been considered as the most secure as whose security cannot be broken down into any means so hypervisor is responsible for all the instances and service scheduled. [18] The other technique is that we can prolong the information that whenever the customer user wants to access the cloud and opens the account and then they can use that information to verify the validity of the new instance of the customer.

4.3 Side Channel Attack: In side channel attack, on the same virtual machine attacker tries to run on the same physical host's and takes the benefit of the physical component in order to steal the information from the fatality. [17] Side channel attacks had come into view that the effective security threat targets the fulfillment of algorithms of cryptographic.

A side channel attack offers the 2 kinds of attacks: [19] VM-CO residence and Placement. Our policy comprises of detecting the attack before it takes place, for eg. If a user tries to launch and ends with a huge number of machines then he would be considered as a potential attacker. In order to pursuit this solution, we require two different elements:[18]

Logs/Events: when a new machine is launched or abort, an event must be generated.

Correlation: Logs are converted into events before they are being delivered.

Solution for Side Channel Attack:

To avoid the cloud from side channel attack usage of virtual firewall appliance will be merged. According to the study of Amazon EC2 it had become possible to personify the new virtual machine to identified targeted virtual machine in the cloud and tries to extract some related information. [17] So therefore utilizing the side channel attacks it becomes very easy to gain the private information from the device so therefore security against the side channel attack should be authenticated.

4.4 Authentication Attack: This type of attack is an inadequate point in the cloud computing services that is often being targeted by the attacker. There are various ways to authenticate the users which can be relied on what actually the user wants.[18] If the data transmitted is confidential then it can categorized as the most possible solution for the secured data information. Nowadays, In addition to this, the accessibility of data process and management for all those data that belonged to the enterprises but they are stored on the user providers instead of the service providers.[17]

Solution for Authentication Attack:

Some services still uses the simple username and password of the authentication based on knowledge but some exceptions are financial institutions that are using the secondary authentication that will make it difficult for the popular phishing attacks. [18]

4.5 Man-In-The-Middle Cryptography Attack: This type of attack occurs when the attacker places himself between the two users. In this when the attacker hinders the messages in the public key exchange and then they retransmit it, and replacing his own public key so that the two original parties appear to communicate with each other.[19] The sender of the message is not able to determinate that the receiver is not known to the attacker and tries to modify the message before re-transmitting to the receiver. Various types of MIM attacks includes: Address Resolution Protocol Communication (ARP), ARP Cache poisoning, DNS spoofing, and Session Hijacking etc.[17]

Solution for Man-In-The-Middle Attack:

This type of attack can be avoided with the help of authenticated process to verify the identity of the customers. So the authentication of users can be effectively and efficiently for the authentication of the users.[17] By using the one time password because one time password is immune to the MIM attack.

5 APPLICATIONS OF CLOUD COMPUTING:

In Cloud computing there are many precisions that are developing, enterprises provides the services in the cloud and they are approachable by others via the internet. The users who offer these services have very brief knowledge of the technology that is being used. [20] The users too do not have much command on the infrastructure that supports the technology being used. Therefore, the applications of cloud computing are practically considered as limitless.

1. Users would be able to authorize their data and applications from anywhere at any amount of time. They can even access the system of cloud computing by using any computer link to the internet.
2. Data would not only be restricted to the hard drive on one's user computer or a internal network.
3. It could even lower the prices of hardware. We don't need to buy the most memory with the fastest computer because system of cloud would be taking care of those needs for us. In lieu of this, we can buy a valuable computer terminal. [21] The terminal can be monitor, any input devices like keyboard, mouse that is mandatory for the cloud system to connect. We don't need to even purchase a large hard drive because we need to store all the information on the remote computer.[20]
4. Applications of cloud had become more ordinary for the use in the office like DaaS (Desktop as a Service) or SaaS. Cloud computing has opened the chance for the reduction of costs licensing.
5. Various digital storage devices and the servers take their space as there is no space available on their site to store the servers and databases so few companies rent the physical space. [20] Cloud computing gives them the opportunity to store the databases and servers on someone else hardware by avoiding the rental physical space on the front end.
6. Many sectors of government are there who are not able to deploy the cloud computing but various projects of pilot are running to interact a geographical difficult to extend the area of country to a capital.[21]

6 CONCLUSION

Cloud Computing is considered as a most important challenge in the information and technology. In respect to the user's confidence, security plays a vital role in the cloud.

In this paper we have discussed about the architecture, security issues related to different layers in cloud. There are various security attacks and their solutions associated with it.

REFERENCES:

[1] Kundu, A; Banerjee, Saha, P; (2012) "*Introducing New Services in Cloud Computing Environment*", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2] Available from http://searchcompliance.techtarget.com/definition/cloud-computing-security

[3] Available from https://www.techopedia.com/definition/72/security-architecture

[4] Available from http://cloudtimes.org/2011 four-layers-of-cloud-computing//05/01/

[5]Availablefromhttp://www.informit.com/library/content.aspx?b=Troubleshooting_Remote_Access&seqNum=139

[6] Available from http://www.cse.wustl.edu/-jain/cse571-11/ftp/virtual/index.html.

[7] Available from http://www.webopedia.com/TERM/I/IP_spoofing.html

[8]Available from https://en.wikipedia.org/wiki/Denial-of-service_attack

[9] Available from https://en.wikipedia.org/wiki/Cloud_computing_security#Ciphertext-policy_ABE_.28CP-ABE.29

[10] Available from http://ac.els-cdn.com/S1877050915007541/1-s2.0-S1877050915007541-main.pdf?_tid=54ce7ee0-fa72-11e6-840a 00000aacb361&acdnat=1487928143_2930317e7fd7eeffb9c0b458d43c7650

[11]Chouhan, P; Singh, R; (2016) "*Security Attacks on Cloud Computing With Possible Solution*"https://www.ijarcsse.com/docs/papers/Volume_6/01_January2016/V6I1-0140.pdf

[12] Hinkle, M. (2010)"Three cloud lock-in considerations", Zenoss Blog.

[13] Padhy, P; Patra, R; (2011) "*Cloud Computing: Security Issues and Research Challenges"* http://www.ijcsits.org/papers/Vol1no22011/13vol1no2.pdf

[14]Prasad, R; Panhale, S; (2013) "*Review of Cloud Computing and Its Application*" http://ijarcet.org/wp-content/uploads/IJARCET-VOL-2-ISSUE-1-290-292.pdf

[15] Rani, D; Ranjan, R; (2014)," *Enhance data security of private cloud using encryption scheme with RBAC*" http://www.ijarcce.com/upload/2014/june/IJARCCE10C%20s%20dimpi_rani%20Enhance%20data%20security.pdf

[16] Rosado, G; Fernandez, B; (2013) "*An analysis of security issues for cloud computing*" http://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5

[17] Sabahi, F; (2012),*" Secure Virtualization for Cloud Environment Using Hypervisor-based Technology"* http://ijmlc.org/papers/87-A888.pdf

[18]Singal, P; Chillar, R.S; (2014) "*A Review on GPS and its Applications in Computer Science*" http://ijcsmc.com/docs/papers/May2014/V3I5201499b17.pdf

[19] Singh, J; Baburaj, E; (2015) "*LAYERS BASED SECURITY ISSUES IN CLOUD COMPUTING*" https://www.ijarse.com/images/fullpdf/201.pdf

[20] Singh, A; Shrivastava, M; (2012) "*Overview of Attacks on Cloud Computing*" https://pdfs.semanticscholar.org/95c0/ae8181bbd949b69d23b5672038fdf4e4a3d7.pdf

[21]Tripathi, A; Beg, R; (2012),*" 'Cloud Computing'- Architecture, Applications and Advantages"* http://www.ijcta.com/documents/volumes/vol4issue1/ijcta2013040106.pdf