Received Date: 03/02/2021 Acceptance Date: 18/02/2021 Publication Date: 28/02/2021

A CASE STUDY ON CLOUD COMPUTING SECURITY TECHNIQUES, SECURITY ISSUES & RESEARCH CHALLENGES

[1]Thummuluru Kavitha, [2]Dr.Thatimakula Sudha
[1]Lecturer in Computer Science, Dept of Computer Science, Loyola Academy, Alwal, Secunderabad, Telangana, India and Research Scholar in Sri Padmavati Mahila Visvavidyalayam, Tirupati, Andhra Pradesh, India.
[2]Professor in Computer Science & Research Supervisor, Dept of Computer Science, Sri Padmavati Mahila Visvavidyalayam, Tirupati, Andhra Pradesh, India.
Email : [1]tkavithaloyola@gmail.com, [2]thatimakula_sudha@yahoo.com

Abstract: *Cloud computing is a technology that uses remote servers on the internet to store, manage and access data online. It uses the combined concept of "software -as-a-service" and "utility computing", and provides various on-demand services requested by end users. There are many benefits of cloud computing technology like fast and effective virtualization, multitenancy, always available and scales automatically to adjust to increase in demand etc. Though it has many benefits to perform different operations but there is an important and critical issue i.e security issue in cloud computing because of the distributed resources. In this paper we firstly list the cloud computing architecture then security techniques used in the cloud computing and about the parameters that affects the security of the cloud then it focus on the security issues of cloud computing and the troubles faced by providers and consumers about their data, privacy, and infected application and threats in cloud computing. It also presents a different research challenge which helps the researchers to focus on those areas.*

Key Words: *Cloud Computing, Data issues, Security issues, Security techniques.*

1. INTRODUCTION:

Cloud computing is a technological advancement that focuses on the way in which we design computing system, develop applications, and leverage existing services for building software. [1] [2]. It is a utility-oriented and internet centric way of delivering IT services on demand [3]. Resources are made available through the internet and offered on pay-per-use basis from cloud computing vendors. Cloud computing cover the entire stack from the hardware infrastructure packaged as a set of virtual machines to software services such as development platforms and distributed application .[4] [5]. Cloud computing supports different operations like:

- Developing new applications and services
- Storage, back up, and recovery of data
- Hosting blogs and websites
- Delivery of software on demand
- Analysis of data
- Streaming videos and audios

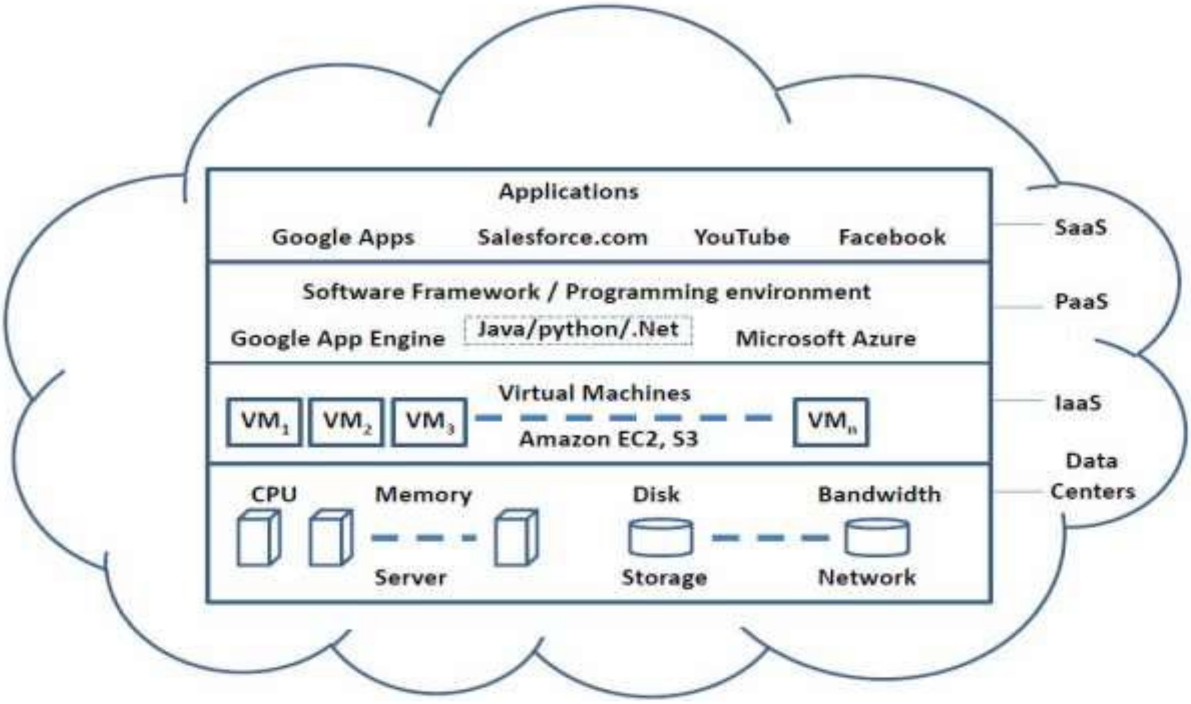
Cloud Computing architecture is divided into two parts:

1. Front End
2. Back End

Both the ends are connected through Internet.

1. **Front End** – It refers to the client part of cloud computing system which consists of interfaces and applications that are required to access the cloud computing platforms. Ex- web browser.
2. **Back End** – It refers to the cloud itself which consists of all the resources needed to provide cloud computing services. It consists of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc. The back end is responsible to provide built-in security mechanism, traffic control and protocols. The server employs certain protocols known as middleware, which help the connected devices to communicate with each other [7].

Cloud providers in general offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). [9]



High Level View of Cloud Computing Architecture

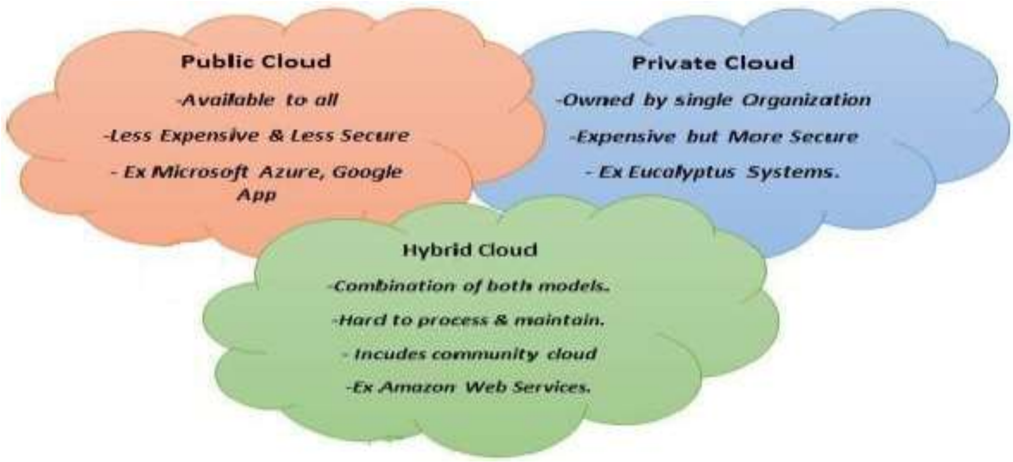
- **Software-as-a-Service (SaaS):** It is a software delivery model providing access to applications through the internet as a Web-based service.
  It provides a means to free users from complex hardware and software management by offloading such task to third parties, who build applications accessible to multiple users through a web browser. In this scenario, customers neither need install anything on their premises nor have to pay upfront costs to purchase the software and the required licences [10]. SaaS is also known as "**On-Demand Software**" in which services are hosted by a cloud service provider.
  Examples of SaaS includes: Salesforce.com, Google Apps.

- **Platform as a Service (PaaS):** "PaaS" provide a development and deployment platform for running application in cloud. It also provides development and deployment tools required to develop applications PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle.
  Examples of PaaS includes: Google App Engine, Salesforce.com, and Cloud Foundry from VMware.
- **Infrastructure as a Service (IaaS):** Infrastructure as a service (IaaS) provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc. Apart from these resources, the IaaS also offers:

  - Virtual machine disk storage
  - Virtual local area network (VLANs)
  - Load balancers
  - IP addresses
  - Software bundles

  Examples of IaaS include: Amazon Web Services, Tata Communications, and Reliance Communications.

Clouds are categorized into different types:-
Public Cloud – The cloud is open to the wide public.
Private Cloud – The cloud is owned by the single organization.
Community Cloud – The cloud is specifically designed to address the needs of a specific industry.
Hybrid Cloud – It is a mixture of public and private cloud, in which the critical activities are performed using private cloud and the non-critical activities are performed using public cloud.


Public Cloud
-Available to all
-Less Expensive & Less Secure
- Ex Microsoft Azure, Google App
Private Cloud
-Owned by single Organization
-Expensive but More Secure
- Ex Eucalyptus Systems.
Hybrid Cloud
-Combination of both models.
-Hard to process & maintain.
- Incudes community cloud
-Ex Amazon Web Services.

2. CLOUD COMPUTING SECURITY ARCHITECTURE AND SECURITY TECHNIQUES:

Securing the cloud starts with the cloud architecture. The cloud computing security architecture is meant to secure and consider an enterprise's data and collaboration application within the cloud through the lens of shared responsibility with cloud providers. The cloud security is based on a model-shared cloud responsibility in which both the provider and the customer possess responsibility in securing the cloud. The cloud providers are responsible to cover many aspects of physical, infrastructure and application security while the cloud customers are responsible for certain areas of security and control, depending on the cloud environment.

IaaS Cloud Computing Security Architecture

This architecture provides the storage and networking components to cloud networking. It depends on application programming interfaces (APIs) to allow enterprises to manage and interact with the cloud. The cloud APIs tends to be insecure as they are open and readily accessible on the network. The CSP (cloud service providers) handles the security of the infrastructure and the abstraction layers. The security issues are visible during the deployment of network packet brokers (NPB) in an IaaS environment.

IaaS cloud computing service models requires additional security features:-

1. Virtual web application firewalls placed in front of a website to protect against malware
2. Virtual network-based firewalls located at the cloud network's edge that guards the perimeter, Virtual routers
3. Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS)
4. Network segmentation

SaaS Cloud Computing Security Architecture

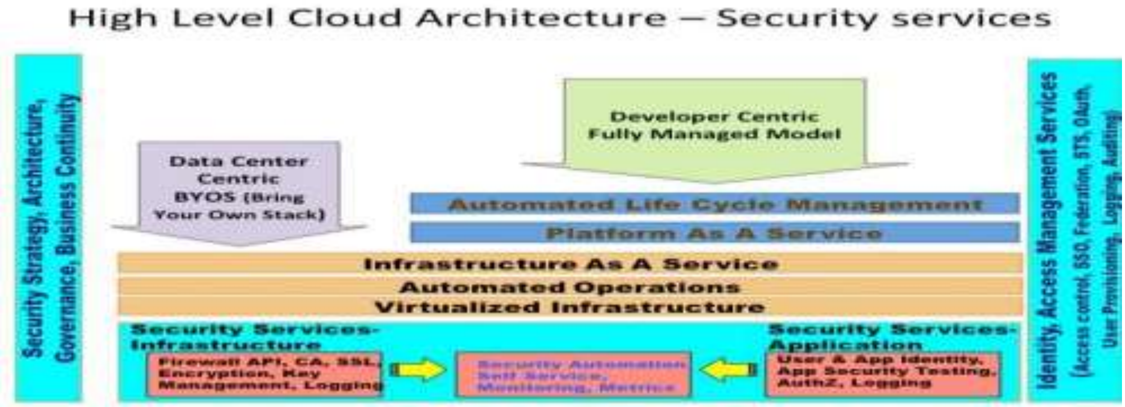
SaaS hosts software and data that are accessible via a web browser. The enterprise normally negotiates with the cloud service provider in terms of security ownership in a legal contract. Cloud Access Security Brokers (CASB) plays a major role in discovering security issues within a SaaS cloud service model as it logs, audits, provides access control, and oftentimes includes encryption capabilities. Security features for the SaaS cloud environment include:

1. Logging
2. IP restrictions
3. API gateways

PaaS Cloud Computing Security Architecture

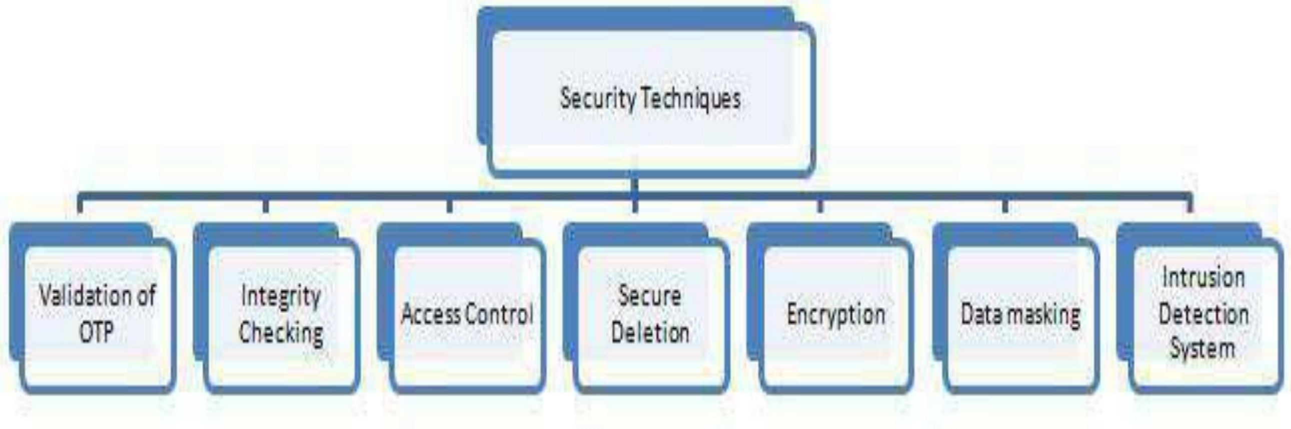
PaaS offers a middleware for developing application together with the infrastructure. Application management is the core functionality of the middleware. The majority of a PaaS cloud service model security is the responsibility of cloud service provider. The security of applications rests with the enterprise. The components to secure the PaaS cloud include:

1. Logging
2. IP restrictions
3. API gateways
4. CASB(**Cloud access security brokers (CASBs)** are on-premises or cloud-hosted software that sit between cloud service consumers and cloud service providers to enforce security, compliance, and governance policies for cloud applications.)


High Level Cloud Architecture – Security services
Security Strategy, Architecture, Governance, Business Continuity
Data Center Centric BYOS (Bring Your Own Stack)
Developer Centric Fully Managed Model
Automated Life Cycle Management
Platform As A Service
Infrastructure As A Service
Automated Operations
Virtualized Infrastructure
Security Services- Infrastructure
Firewall API, CA, SSL, Encryption, Key Management, Logging
Security Automation Self Service, Monitoring, Metrics
Security Services- Application
User & App Identity, App Security Testing, AuthZ, Logging
Identity, Access Management Services
(Access control, SSO, Federation, STS, OAuth, User Provisioning, Logging, Auditing)

SECURITY TECHNIQUES FOR SECURING CLOUD:

Cloud data encryption does not provide the solution for data which can keep faith over cloud security. Along with encryption there are many security techniques are available to secure the data in cloud. The following Figure explains security techniques.



Security Techniques for Securing Cloud

A. Validation of OTP

In the current scenario, many of banks are providing authentication through a One Time Password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. This is used by many online platforms to validate the cloud users. In some cases it is used for two time authentication called as Multiple Authentication Factor.

B. Integrity Checking

The integrity of cloud data is a guaranteed as the cloud data can only be changed or accessed by an authorized user. In simple terms, it is a cloud-based data verification process ensures that the data is unmodified, correct and the basic techniques of data integrity are Provable Data Possession (PDP) which ensures the integrity of cloud data on a remote server and the technique Proof Of Retrievability (POR) is used to obtain and verify the evidence that cloud data is stored by the user on the server is not changed [13].

C. Access Control

Access control means cloud data owner can execute some restrictive permission to access their data outsource to cloud and data owner's authorized user can access cloud data while unauthorized user can't due to access control cloud data are protected from modification or unauthorized disclosure of data.

D. Secure Deletion

Secure deletion is done using different techniques like Clearing; in this technique we delete the media before the reuse of these media and at the same time provide protection for accepting the data that contained in the media before deleted. Sanitization, here the protection for accepting previous data is not provided and this type of data is regularly circulated for lower level of classification [14].

E. Encryption

Cloud security provides data encryption service to encrypt cloud data before transfer from local storage to cloud storage and it is impossible to understand from any system, database or file to decrypt data without decryption key and encrypted data is only possible to access with an authorized user with the decryption key and separation of encrypted data and encryption key is necessary for keeping cloud data secure.

F. Data Masking

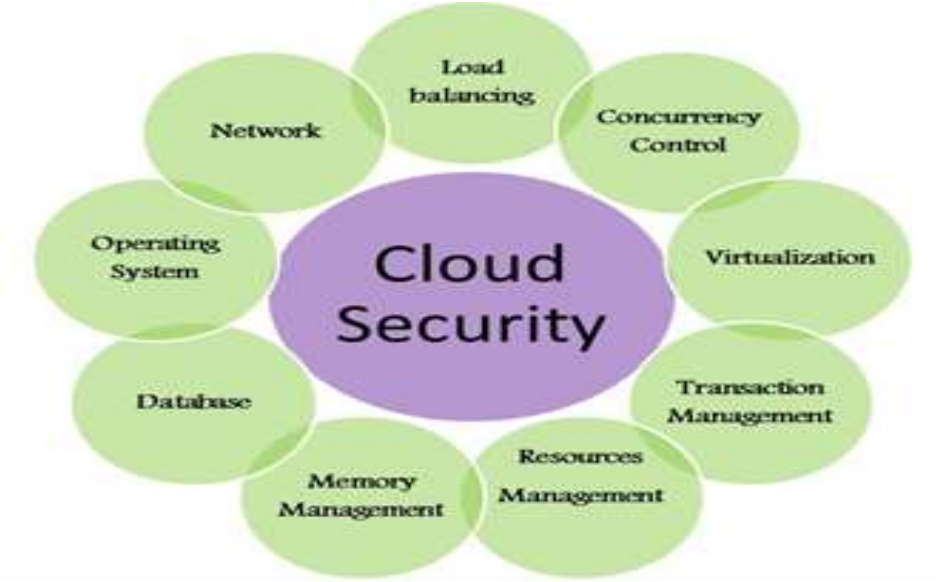
Data masking is a process of securing and hiding cloud data from attackers and theft which insure that the information is changed with realistic but not real information. There are different ways or methods are used to mask cloud data, Static Data Masking (SDM) is used by most organizations when creating tests and this is actually the only method of masking possible when using outsourced developers in a separate site or company. In such cases, it is necessary to duplicate the database. Dynamic Data Masking (DDM) provides access based on their role in the organization [15].

G. Intrusion Detection System

Intrusion Detection System (IDS) defines as a software applications or devices that keep eyes on system activities or network traffic and find if any illegal activities occurred. In the recent era, most of the hackers use different attacking techniques for finding users sensitive information. An intrusion represents illegal activities for IT resources. The intruders try to find unauthorized access in sensitive information, causes harmful activities. The two types of Intrusion Detection System are defined, Network-Based Intrusion Detection System (NIDS) that present in a devices or computer connected segment of an organization’s network and monitor network traffic and keep eyes on on-going attacks, Host-Based Intrusion Detection System (HIDS) is installed on specific system or server and monitor illegal activities on that system.

3. PARAMETERS AFFECTING CLOUD SECURITY

The cloud computing features are very appealing but nothing is perfect. Because the Cloud computing got many security issues especially on Data theft, Data loss and Privacy [7], [8].This paper lists the different parameters that can affect the security of the cloud and also explores the cloud security issues and problems that the cloud computing service provider and also the cloud service customer face. There are many security issues for cloud computing as it is surrounded with many technologies that include networks, operating systems, databases, resource allocation, transaction processing, virtualization load balancing, memory management and concurrency control[6] [8].



Parameter that affects cloud security

THREATS IN CLOUD COMPUTING

A. Data breaches

Cloud environments face many of equivalent threats as traditional corporate networks, but since a huge amount of data is stored on cloud servers, providers have become an attractive target. The severity of the damage depends on the sensitivity of the data that is exposed. Maximum percentage of breached records comes from government, retail and technology industries as they are very popular targets because of the high level of personal identifying information contained in their records. A company may be subjected to legal action when a data breach takes place. Breach investigations and customer notifications can rack up significant costs and indirectectly effects brand damage and loss of business which can impact organizations future for years.

B. Exploited system vulnerabilities:

Within a CSP's infrastructure, platforms or applications that support multi-tenancy can lead to a failure to maintain separation among tenants when exploitation of system and software takes place. This provides a way to the attacker to gain access from one organization's resources to another user's or organization's assets or data. Multi-tenancy increases the attack surface, thus increases the chance of data leakage if the separation control fails. This type of attack can be accomplished by exploiting vulnerabilities in the CSP's application, hypervisor or hardware.

C. DoS (Denial-of-Service) attacks:

In cloud computing DoS is an attack during which the perpetrator seeks to form a network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the network. It compromises the availability of the cloud resources and services often target the computer network's bandwidth or connectivity. Systems may run slow. DoS attacks consume huge amounts of processing power, a bill the customer may ultimately have to pay. High-volume DoS attacks are quite common, but organizations should even be conscious of asymmetric and application-level DoS attacks, which target Web server and database vulnerabilities.

D. Permanent data loss:

Data stored in the cloud are often lost for reasons apart from malicious attacks. Accidental deletion of data by the cloud service provider or a physical catastrophe, like fire or earthquake, can cause permanent loss of customer data. So adequate data backup measures and disaster recovery are vital, daily data backup and off-site storage are vital with use of cloud environments. The burden of avoiding data loss doesn't fall solely on the provider's shoulders. If a customer encrypts its data before uploading it to the cloud but loses the encryption key, the data are going to be lost. Losing such sensitive data may have serious consequences.

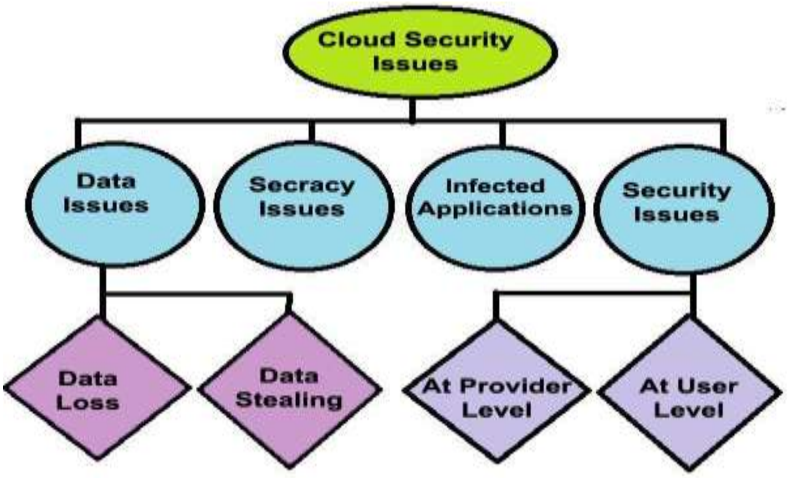
E. Inadequate diligence:

Organizations accepting cloud computing without having complete understanding of the environment and risks associated with it going to encounter a great number of economic, financial, technical, legal, commercial and compliance risks. Diligence is required whether the organization is trying to migrate to the cloud or merging with another company within the cloud. For instance, organizations that fail to look at a contract might not remember of the provider's liability in case of data loss or breach. Operational and architectural issues could arise if an organization development team isn't conversant with cloud technologies as apps are deployed to a specific cloud. An organization should do adequate research before moving to cloud computing due to the risk related to it.

VARIOUS SECURITY ISSUES FACED BY CLOUD COMPUTING:

The cloud computing service providers should make certain that their customers shouldn't face any type of problem namely loss of their important data or data theft. At cloud computing there could also be an opportunity where an unauthorized user can infiltrate the cloud computing by impersonating a legitimate user, there by infect the whole cloud with a virus. This result can affect many customers who are sharing the infected cloud [7]. There are four issues associated with the security of cloud computing.

a. Data Issues
b. Privacy issues
c. Infected Application
d. Security issues



Security Issues of Cloud Computing

A. Data Issues*:*

In a cloud computing environment sensitive data arise as a significant issue regarding to security in cloud computing based systems. Firstly, when the data is in cloud, anyone can access data from anywhere and anytime from the cloud because the data could also be usual, private and sensitive data in a cloud. During the same time, many cloud computing service customers and providers are accessing and modifying the data. So there’s a crucial requirement for data integrity method in cloud computing environment. Secondly, the data embezzlement is another serious issue in cloud computing environment. As we say that a lot of cloud computing service providers don’t have their own servers, they buy the servers from other service providers thanks to it is cost effective. So there is a probability that data are often stolen from the external servers. Thirdly, Data loss may be quite problem in cloud computing environment. Cloud computing service providers whenever close their services due to some financial or legal issues then there will be a loss of data for the customers. Moreover, data are often damaged or corrupted due to some miss happening, natural disaster, and fire. Due to above condition, data might not be accessible to the cloud computing service providers customers. Fourthly, data location is additionally a crucial and customary security issue that needs focus with in the cloud computing environment. Because the physical location of data storage is extremely important and crucial in the cloud computing.

B. Secrecy Issues:

The service providers of cloud computing should kept in mind that the customers important information is fully secured from other service providers, customer and user because the most of the cloud servers are external. The cloud service provider should make it clear about who is accessing the data and also keep it well clear that who is maintaining the server in order that it’ll help to the provider to secure the customer’s personal data.

C. Infected Application:

The cloud computing service providers should have the entire control and access to their servers, in order that they will monitor and maintain their servers. This may cause the hindrance to the malicious user from uploading any virus affected application onto the server which can seriously affect the user and cloud computing service.

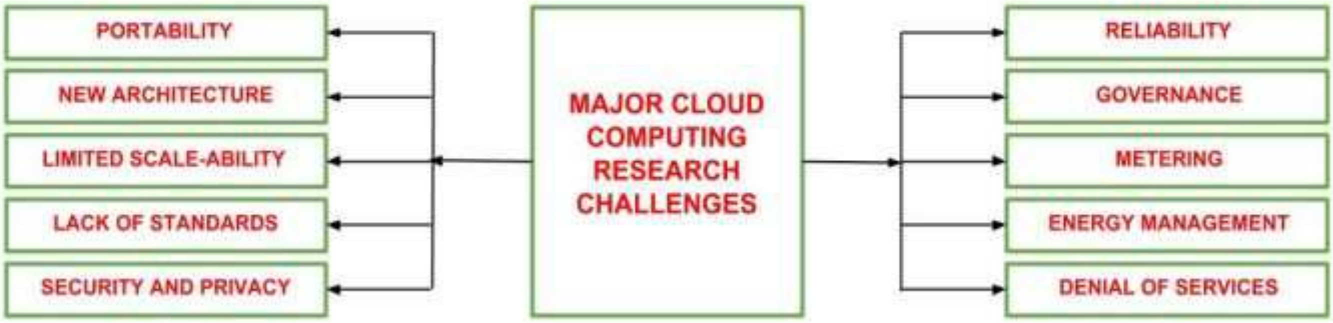
D. Security issues:

The security of cloud computing must be done on both sides i.e. cloud computing service provider’s side and therefore the customer’s side. The Cloud computing service developers should be fully sure that their server is secured from all the surface environmental threats which will arise with in the cloud. They ought to provide a good security layer to their customers; before using the services of cloud computing the user should also confirm that there shouldn’t be any type of data loss or theft or tampering of data for other customers who are within the same cloud. A cloud is efficient only when there is a good security mechanism provided by the service provider to its consumers.

4. RESEARCH CHALLENGES:

Cloud Computing has many benefits and it is adopted by many companies and industries, the research on cloud computing is still going on there are many existing issues haven’t been completely addressed, while new challenges keep on emerging from industry applications. A number of the challenging research issues in cloud computing are given below.

- Portability
- Development of latest architecture
- Limited scalability
- Lack of standards
- Security of privacy
- Reliability
- Governance
- Metering
- Energy management
- Denial of service



- **Portability-** Portability is that the ability to manoeuvre application and its data from one place to a different. It's achieved by restricting dependencies on the underlying platform. The portable component which consists of application and data might be moved and reprocessed regardless of the provider, platform, operating system, location, storage etc. e.g., if the old cloud environment is Windows and new cloud environment is Linux then an application running on old cloud would be ready to run on new cloud without being changed is named portability.
- **Development of latest architecture-** Currently, most of the cloud computing services are employed in huge commercial data centers and that they are functioned in old centralized manner. This approach has its own benefits, i.e., economy of scale and high manageability, though it has some limitations. This model of cloud computing during which using voluntary resources, or a mix of both dedicated and voluntary resources are very reasonable and it suits such applications as scientific computing. Though, no matter it has advantages, yet this architecture has open research challenges also in the form of heterogeneous resources management.
- **Limited scalability–**Cloud computing service providers promise to deliver infinite scale-ability for customer but thanks to the very fact that many users are now migrating to cloud computing so such promise isn't fulfilled. The challenge of availability and scale-ability presents another research area for the researcher to seek out an optimum solution for these problems.
- **Lack of standards –** Each cloud services provider has their own standards and no comparative performance measurement facility is available to the user by which he can compare standards and performance. It's still needed that cloud computing should be standardized.
- **Security of privacy –** The most obstacle within the fast adoption of cloud is that the security apprehensions of the customers. While thanks to the support of recent techniques of security the possibilities of security flaws are reduced but still, when worms and hackers attack a system, disorder is made within a couple of hours. It's essential that the applications and architectures should be private and therefore the mechanism of security must be relevant, evolving and adoptive. Trust and Privacy are another possible areas of research in cloud computing.
- **Reliability –** When it involves availability of connection to cloud network but it becomes a problem. User's isn't sure if he will remain connected to cloud network and can continue his work on at any time as connection is lost. The connections to cloud services are secure or not and therefore the movement of data to cloud computing is in safe environment and as per needed speed or not. Is the cloud itself is reliable enough to be migrated to? So, reliability is another challenge.
- **Governance –** Many administrations started providing cloud services using their own data centers, thus trying to control and convey authority in cloud computing. Governments, organizations and users must get to work together to resolve this issue.
- **Metering –** Administrations using cloud services must meter and monitor the performance of services. Cloud services providers must provide a facility to measure and monitor their services across standard parameters.
- **Energy management –** The prerequisite of the cloud computing is that the management of various resources across a distributed computing environment. By the user's perspective all these resources are? "On all the times". If this is often the case, then, it's highly unproductive in terms of the need for the energy consumption. A lot of research has been carried out in developing energy efficient equipment and utilize this equipment in building data centers to be energy efficient thus protecting the environment with less carbon emission.

- **Denial of service –**Another trending issue and a challenge that's faced by the researchers is that the denial of service (DoS) in cloud computing. As a matter of fact, cloud provides the allocation of resources dynamically, so what is going to be the response of the cloud when it's under a heavy denial of service attack? Is it necessary to create a Denial of Service protection into cloud or it'll be handled on the internet level as it is dealt now? This also poses another challenge for the researcher.

5. CONCLUSION:

The cloud computing service provider and the consumer both should be fully sure about that their cloud is fully protected from all the external threats or attacks. The largest gap between cloud security applications and research theory lies in the fact that the assumption in the research leaves some important differences among the actual cloud security and the virtual machine security. Research should be centre on these gaps and differences and its removal. One of the major security problems with the cloud computing model is the sharing of resources. Cloud service providers are responsible to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security architecture, security techniques, security issues and research challenges in cloud computing. Data security is major issue for Cloud Computing. This paper has focussed all these issues of cloud computing. The complexity of the cloud design makes difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be modified which can perform well with the clouds architecture.

REFERENCES

1. Michael Glas and Paul Andres, "An Oracle white paper in enterprise architecture achieving the cloud computing vision", CA-U.S.A, Oct 2010.
2. Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework fore management of NGO's", IJoAT, ISSN 0976-4860, Vo l 2, No 3, Department Of Computer Science, Eternal University, area is Cloud Computing, Software Engineering, and Data Mining. Baru Sahib, HP, India, July 2011.
3. Dr. Gurdev Singh, Shanu Sood, Amit Sharma, "CM -Measurement Facets for Cloud Performance", IJCA, ,Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.
4. Joachim Schaper, 2010, "Cloud Services", 4th IEEE International Conference on DEST, Germany.
5. Tackle your client's security issues with cloud computing in 10 steps, http://searchsecuritychannel.techtarget.com/tip/ Tackle-your-clients-security-issueswithcloud-computing-in-10-steps.
6. T.Kavitha "A brief on cloud computing security issues and solutions" 2018 IJRAR nov 2018, volume 5, issue 4, E-ISSN 2348-1269, P-ISSN 2349-5138.
7. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(S.Kuppuswamy, P. B. Shankar Narayan, "The Impact of Social Net working Websites on the Education of Youth", In International Journal of Virtual Communities and Social Networking, Vol. 2, Issue 1, page 67-79, January-March 2010.
8. http://searchvirtualdatacentre.techtarget.co.uk/news/1510 117/Community-cloud-Benefits and-drawbacks
9. A. Kundu, C. D. Banerjee, P. Saha, "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.
10. R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
11. B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.
12. 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.
13. S. Sharma, "Data Integrity Challenges in Cloud Computing", 4th international conference on recent innovations in science engineering and management, pp. 736-7436, 2016.
14. Cloud Codes [online] https://www.cloudcodes.com/blog/ data-protection-controls-techniques.html (Accessed 20 December 2019).
15. G.K. Ravikumar "Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing", *International journal of engineering science and Technology*, vol. 3, no. 6, pp. 5150-5159, 2011.

16. X. Zhang, N. Wuwong, H. Li, and X. J. Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments", In Proceedings of 10th IEEE International Conference on Computer and Information Technology, pp. 1328- 1334, 2010.
17. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4
18. Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing," 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010. ISBN: 978-1-4244-8567-3.
19. S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing"; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084-8045.
20. V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.