International Journal of Research in Advent Technology, Vol.6, No.12, December 2018
E-ISSN: 2321-9637
Available online at www.ijrat.org

To study Security Challenges and Vulnerabilities in Cloud Computing

Dr. K.Vaishali [1], Mrs. Saroj A. Shambharkar[2]
Principal, Jyothishmathi Institute of Technological Sciences, Karimnagar[1], Information Technology[2], Kavikulguru Institute of Technology and Science, Ramtek
Email: saroj.shambharkar@gmail.com

Abstract- - Cloud computing associated with applications and services that run on a distributed network using virtualized resources which accessed through the common IP and networking standards. It is prominent by the notion that resources are virtual and limitless. Cloud computing has attracted more attention due to its high cloud services demand by the people all around. The huge scale of cloud computing systems was empowered by the popularization of the Internet and the growth of some large service companies. It provides an opportunity to pay less and grow fast. The details of the physical systems on which software runs are abstracted from the user which became the most efficient option without any initial investment and day by day frequent and heavy use of cloud computing are increasing along with its benefits, accessing a cloud services imposes certain security challenges which are associated under a cloud computing platform environment used by the organizations. So, they have to be known and to be resolved. The security challenges are layers dependency stack, multi-tenancy, model architecture, and elasticity. The users of Cloud computing services encounter threats of security by internal and external sources. In this paper, we introduce a detailed analysis of the seven cloud security challenges identified and discussed the corresponding solutions of them.

Index Terms- Cloud Computing Service, Distributed Computing, Cloud Security Controls

1. INTRODUCTION

A Internet become the part of human being from last few decades it's the rapid development of the computer and modern communication technology which brings enormous changes in our lives. Every day due to increase in the demand more efficient, productive and economical resources is necessary to sustain the large amount of data. Cloud computing is progressively investigated and adapted, which will resulting profound changes in IT industry, but it will also bring enormous impact as well as challenges to end users information and privacy protection.

The National Institute of Standards and Technology (NIST) defined the term cloud computing as: "Cloud computing is a way of enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]."

Although the cloud computing has been studied and applied only a few years, the development of cloud computing is very fast. In other countries, the cloud computing technology has been the new strategic core by some international well-known IT companies. Gartner Company has put cloud computing at the first grade in the future ten strategic technologies of IT for two consecutive years. Meanwhile, IT companies like the Amazon, Google, IBM and Microsoft, have launched their own cloud computing infrastructure and cloud services on the basis of their original products, and achieved good application results and social impact, such as Amazon's EC2 and S3,Google Apps, Microsoft' Azure, IBM's Blue Cloud and so on.

Cloud computing still faces problems related to security threats from internal and external sources though it has more powerful and reliable capabilities for management and has reliable cloud computing system infrastructure. There are many examples of security breach in the recent times like Apple's iPad subscriber privacy leak , Amazon S3's recent downtime [2], and Gmail's mass email deletions (27). Cloud service provider organizations usually don't examine data sent or received by user to the cloud and users don't have any access to the internal procedures of a cloud, hence leading to possibility of data breach. Additionally, owing to hardware virtualization, multiple users can now share the same physical infrastructure, which runs their distinct application instances simultaneously. From user point of view cloud computing seems to be very insecure due to privacy and security vulnerabilities arises from its multi-tenancy feature [3]. It is not possible for user to get control of his data and computing applications until a strong security measure and privacy guarantee are not in place. User will not give priority to scalability,

flexibility and economic availability over its privacy and security of his personal data. More motivation is required towards addressing security issues and providing more trustworthy solutions for making a cloud more helpful and accessible to public at large. data and privacy security. Last year, Google Gmail email up broke down for 4 hours in the global scale, Microsoft's cloud computing platform Azure was out of service for about 22 hours. Despite the potential benefits and revenues that could be gained from the cloud computing model, the model still has a lot of open issues that impact the model creditability and pervasiveness. Vendor lock-in, multi-tenancy and isolation, data management, service portability, elasticity engines, SLA (Service Level Agreement) management, and cloud security are well known open research problems in the cloud computing model. The security risks of cloud computing is growingly concerned about.

The present study focuses on the safe implementation of the cloud based computing infrastructure and to address issues of secure usage of this new facility. Various security issues involved in cloud computing implementation have also been discussed and discussion regarding the authentication of cloud computing has also been taken care of with a view to keep integrity in security of cloud computing.

2. CLOUD COMPUTING

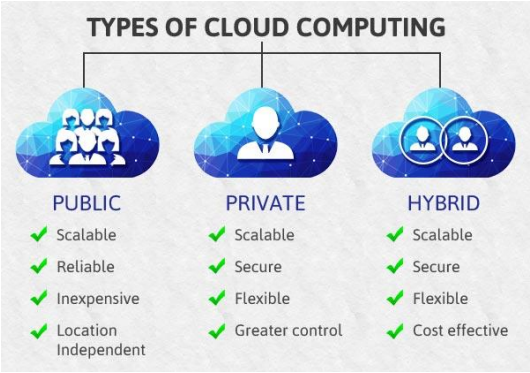

Fig 1.1 Types of Cloud Computing

2.1. Types of Cloud Computing

Cloud computing is divided into three types Private Cloud, Public Cloud and hybrid cloud.

Private Cloud: The cloud is deployed by the private Companies for its own purpose and may be sometimes their own premises. This type of cloud provides limited access for specific group. Services are design for private benefits called as private cloud that can be one house, industry cloud.

Public Cloud: This type of clouds is implemented for general Purpose. These are generally available in internet and provided for use on rent basis to the public. This can be accessed by any user and charges are applied to the client on behalf of service utilization.

Hybrid Cloud: The types of clouds are generally a combination of the private cloud and public. This is used when private cloud needs some special service from public cloud.

2.2. Cloud Computing Challenges

Data Security Challenges As we are moving into internet based cloud model, it requires great emphasis on Data Security and Privacy. Data loss or Data leakage can have severe impact on business, brand and trust of an organization. Data leak prevention is considered as most important factor with 88% of Critical and Very important challenges. Similarly Data Segregation and Protection has 92% impact on security challenges

Here we ranked the top data security challenges that have their impact on business, brand and trust of an organization:

2.2.1. Data Protection

Protection of Data is that the most vital challenge in cloud computing. once multiple organizations share resources there's invariably a risk of knowledge misuse. To avoid such risk it's necessary to secure knowledge repositories. to boost the safety in cloud computing, it's vital to supply authentication, authorization and access management for knowledge hold on in cloud.

2.2.2. Locality

In cloud computing, finding the location of data is very difficult as it is distributed over the number of regions. When the data is moved to another location the laws applied on that data will also changed. So there is an issue of compliance and data privacy laws in cloud computing. Customers should know their data location and it is to be intimated by the service provider.

2.2.3. Integrity

The system should provide a security mechanism such that data can be only modified by the authorized person. In cloud system, data integrity must be maintained correctly to avoid the data lost. In general every transactions in cloud computing should follow ACID Properties to preserver data integrity.

*2.2.*4. *Access*
Data access principally refers to the information security policies. In a corporation, the workers are going to be given access to the section of knowledge supported their company security policies; the identical information can't be accessed by the opposite worker operating within the same organization. The numerous cryptography techniques and key management mechanisms are accustomed make sure that information are shared solely with the valid users. The key's distributed solely to the licensed parties victimization numerous key distribution mechanisms. To secure the information from the unauthorized users the information security policies should be strictly followed. Since access is given through the net for all cloud users, it's necessary to supply privileged user access. User will use encoding and protection mechanisms to avoid security risk.

*2.2.*5. *Confidentiality*
Data can be placed with the single or multi cloud providers. When data is stored in the remote server, data confidentiality becomes the important requirements. To maintain confidentiality data understanding and its classification, users should be aware of which data is stored in cloud and its accessibility.

*2.2.*6. *Breaches*
Data Breaches is another necessary security issue to be focused in cloud. Since massive knowledge from numerous users are stored on the cloud, there's an opening of malicious user coming into the cloud specified the whole cloud surroundings is prone to a high value attack.

*2.2.*7. Storage
The data stored in virtual machines creates several problems one of such issue is the reliability of data being stored. Virtual machines need to be stored in a physical infrastructure which may cause a potential security risk.

*2.2.*8. *Data Center Operation*
In case of data migration, transfer or in case of disaster organizations using cloud computing applications need to provide security for user's data without any loss. When data is not managed properly, there is an issue of data storage and data access. In case if disaster happens, the cloud providers are fully responsible for the loss of data.

3. CLOUD COMPUTING SECURITY ISSUES

Cloud computing is a way of accessing resources and service for a particular organization. But hacker, attacker and security researcher find out that cloud computing is not fully secure. It has some issues which are mentioned below:

- **Insecure Interface:** Cloud service provider show all the interface and application which is used by the client to interact with cloud. Data arrangement, identity management, monitor of service all happen on the cloud. And authentication and access control is monitored by these interfaces too.

- **Data Loss or Leakage:** When cloud computing is being used. There are two main changes happens to the client data. First one, data is stored away from the client machine. Secondly, data is transmitted from one execution mode to multi execution mode. When these changes takes place the security issue of data loss or leakage is become the prime concern.
- **Malicious Insiders:** At now, cloud is served by organization that hires staff for providing service to its consumer. thus those worker will ill-used data or will sell information to different organization and this is often happen on internal level of an organization and onerous to aware for purchasers or customers.
- **Shared Technology:** components of working under the cloud which make environment (virtual memory, processor, caches etc) for computing does not support strong isolation for multi execution mode.
- **Flood Attacks:** Using the cloud computing services and customer need to extend size of service and initialization is happen due to dependency on internal communication. And attacker makes large false request to the server. So server gets busy and unable to provide services properly.
- **IP Spoofing:** IP spoofing is understood as analysis of network traffic. Once any offender send message to a pc being a sure user. The offender determines the IP address of a sure system and makes some modification to packet data like packet header and sends that packet that looks as packet is originating from sure system.
- **DDOS Attacks:** In DDOS (Distributed Denial of Service) attack, attacker tries to make server busy by sending large number of requests. Due to large number of requests the server gets busy and not able to response on the valid and authentic request of customer. As a result server denies for giving the service to customer and DDOS take place.

- **Malware Injection**
Malware injections are scripts or code embedded into cloud services that act as "valid instances" and run as Software as a Service to cloud servers.

This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves. Once an injection is executed and the cloud begins operating in tandem with it, attackers can eavesdrop, damage the integrity of sensitive information, and steal data.

- **Abuse of Cloud Services**
  The enlargement of cloud-based services has created it potential for each small and enterprise-level organization to host immense amounts of information easily. However, the cloud's unprecedented storage capability has conjointly allowed each hackers and licensed users to simply host and unfold malware, illegal software and different digital properties.
  In some cases this practices affects each the cloud service supplier and its user, as an example, privileged users will directly or indirectly increase the protection risks and as a result infringe upon the terms of use provided by the service supplier.

- **Insecure APIs**
  To customize their cloud experience users can use Application Programming Interfaces (API) However, These APIs can be a potential threat to cloud security as they have their very nature. Not only do they give companies the ability to customize features of their cloud services to fit business needs, but they also authenticate, provide access, and effect encryption.
  As the infrastructure of APIs grows to provide better service, same time it also grows its security risks. APIs give programmers the tools to build their programs to integrate their applications with other job-critical software. A good example of an API is YouTube, where developers have the ability to integrate YouTube videos into their sites or applications.
  The vulnerability of an API lies in the communication that takes place between applications. While this can help programmers and businesses, they also leave exploitable security risks.

4. COUNTER STEPS TOWARDS SECURITY

The main parts of a crypto graphical storage service which might be enforced by employing a completely different techniques, out of that, some were designed specifically for cloud storage. Within the starting of the Cloud Computing, common cryptography Technique like Public Key cryptography was applied. This ancient technique doesn't offer expected result because it support one to at least one cryptography sort communication. Public Key cryptography isn't extremely ascendable. This gave rise to maneuver forward to some advanced cryptography ways. The advanced crypto graphical ways includes the below cryptography ways

• Searchable Encryption: In this we are having two types:-
  1) Symmetric searchable encryption
  2) Asymmetric Searchable Encryption (ASE).
• Homomorphic Encryption
• Identity Based Encryption

4.1 Searchable Encryption

A searchable encryption it is used at high level in order to encrypt the content that is available in search index so that it can hidden from others except the party that provide the authorized tokens A collection of files which consists of full-text index otherwise keyword index considered to generate a search index. The index
is encrypted based on searchable encryption scheme in such a way
(i) The pointers to the encrypted files can be retrieved based on the tokens given for the keyword.
(ii) If the token is not provided then the contents are hidden for the index. However, with the complete understanding of secret key, the tokens are generated.
The retrieval procedure does not reveal the content of the files or the keywords apart from the files that comprise the keyword in common. The previous statement is worth taking about since it is difficult to understand the searchable encryption that is applicable for security.

4.1.1 Symmetric Searchable Encryption

It is suitable for the environment where the client that searches the data and also he is responsible for generates it. A Single Writer/Single Reader (SWSR) is derived from cloud storage terminology. SSE has two major advantages they are efficiency and security. It also has disadvantages such as functionality and tradeoff efficiency.

4.1.2 Asymmetric Searchable Encryption (ASE)

This scheme is suitable for the environment where the client that searches the data is different from the one who generates it. This scenario is referred as Many Writer/Single Reader (MWSR).

4.2 Homomorphic Encryption

In this form of cryptography specific mechanism performs some specific task on encrypted knowledge that isn't offered with different cryptography schemes. Using this any user can encrypt his data and store in

the cloud and later can perform any process without converting the encrypted data

These security issues of data stored in cloud can be resolved by using Fully Homomorphic Encryption (FHE) schemes. To secure it, before being sent to the cloud the data should be encrypted with FHE. First, the user login and uses the key-generation provided by the server to generate the secret key, the user is the only owner of this secret key. Then, the user encrypts the data that wants to send it to the cloud. During transmitting, the integrity and non-repudiation can be assured by applying other cryptographic technologies such as digital signature. When the user want the server to execute some computations on these encrypted data (such as search), he can send encrypted request to the cloud server. The server performs the required operations and sent the encrypted result to user. Finally the user decrypts the data with his secret key to retrieve the correct result

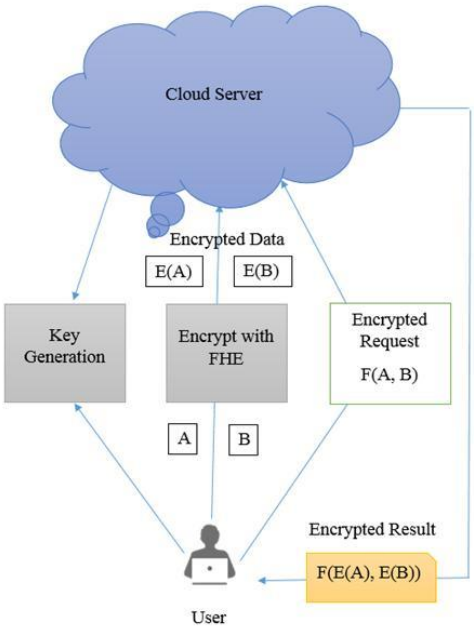

Figure 4.1 Fully Homomorphic Encryption

4.3 Identity based Encryption

In Identity primarily based cryptography, AN identity of the user plays an important role. The sender WHO sends the message solely must understand the receiver's identity attribute so as to send the encrypted messages. Email cryptography is one in every of the key applications for Identity primarily based cryptography. However, key revocation isn't achieved in Identity primarily based cryptography.

4.4 Proofs of storage

It is a sort of service level agreement between the Cloud Service supplier and its users to make sure that the information kept within the servers of cloud computing facility can ne'er be tempered or used while not the permission of the user and guarantees regarding the integrity of knowledge keep in cloud.

4.5 Server Aided Secure Computation

Some computational process is administrated on the encrypted information by server and user collectively without knowing the details of the original data and both the parties remain totally not aware of the process which is going to perform over the data and the outcome achieved.

4.6 Possible solutions against malware injection attacks

We can combine the integrity with hardware to prevent cloud from malware injection attack or can use hardware for integrity purpose because for an attacker it is difficult to enter in the IaaS level. For this we can utilize a file allocation table (FAT) system, by using it we can determine the validity and integrity of new instance by comparing the current and previous instance. For this purpose, we need to deploy a hypervisor on the provider's side. In cloud system hypervisor is considered to be the most secure and efficient part of it whose security cannot be broken by any way. We can enable the hypervisor so that it can check file allocation table to validate and integrate an instance of customer. It is also responsible for scheduling all the instance and services. Another way is that we can maintain the information of the platform type version that a customer user to access the cloud in first phase when a customer open an account and can use those information to check the validity of new instance of the customer.

4.7 Deal with TP spoofing

- Use authentication based on key exchange between the machines on your network; something like IPsec will significantly cut down on the risk of spoofing.

- Denying private IP addresses on your downstream interface by using an access control list.
- Implementing filtering of both inbound and outbound traffic.
- By Configuring routers and switches if they support such configuration, to reject packets originating from outside your local network that claim to originate from within.
- Enable encryption sessions on your router in order that sure hosts that are outside your network will firmly communicate together with your native hosts.

5. CONCLUSION

From the above study we say, Cloud computing is a way of computing which depletes the boundaries of hardware and software. This platform provides a cost effective mechanism to share hardware and software with pay as peruse facility. It is the future trend of IT industry. The popularity of cloud computing, more and more security issues presented in front of us, limiting the popularity of cloud computing. When security & privacy comes into existence then there will many challenges and issues faced by the users such as network security, data security, locality in SaaS models, host intrusion in PaaS and IaaS. Also, according to hackers, crackers and security researcher's suggestion about the cloud computing is that it is not hundred percent safe due to information leakage may happened at any level of cloud. Therefore adoption of cloud computing system as a necessity is always under threat from security issues and requires the safety towards the data breach. In the upcoming year cloud computing can become the front runner for a secure, flexible, scalable, cost effective and virtual, user friendly tool for information technology enabled services but this need to be implemented with proper security mechanisms like cryptography.

REFERENCES

[1] Priyanka Chouhan, Rajendra Singh (2016): Security Attacks on Cloud Computing With Possible Solution", Volume 6, Issue 1, ISSN: 2277 128X.

[2] Bessani A, Correia M, Quaresma B, et al. DEPSKY(2011): dependable and secure storage in a cloud-of-clouds. 6th Conferenceon Computer Systems (EuroSys'11). 2011. p. 31–46

[3] R. Kirubakaramoorthi* , D. Arivazhag anand D. Helen (2015): " Survey on Encryption Techniques used to Secure Cloud Storage System", Vol 8(36), DOI: 10.17485/ijst/2015/v8i36/87861, ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645.

[4] http://techcrunch.com/2010/06/15/ipad-breach-personal- data.

[5] T. Ristenpart et al., (2009): Hey, You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security (CCS 09), ACM Press, 2009, pp. 199–212.

[6] Computing Security in High-speed Railway", IEEE International Conference on Electronic & Mechanical Engineering and Information Technology, Vol. 8, pp. 4358-4363, August 2011.

[7] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser.(2009): Business Models in the Service World." IT Professional, vol. 11, pp. 28-33.

[8] Akhil Bhel,(2011): Emerging Security Challenges in Cloud Computing. Information and Communication Technologies, in: 2011 World Congress on, Mumbai,.p.217-222.

[9] Patil DH, Bhavsar RR, Torve AS.(2012): Data security over cloud.IJCA Proceedings on Emerging Trends in Computer Science and Information Technology (ETCSIT-2012) etcsit 1001.; ETCSIT (5):11–4

[10] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser (2009): Business Models in the Service World." IT Professional, vol. 11, pp. 28-33, 2009

[11] Kresimir Popovic and Zeljko Hocenski.(2010): Cloud computing security issues and challenges, in: MIPRO, Proceedings of the 33rd International Convention, p.344-349

[12] Global Netoptex Incorporated, "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[13] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[14] https://cloudsecurityalliance.org/csaguide.pdf.

[15]Kim Kwang Raymond Choo, "Cloud computing: Challenges and Future Directions", Trends & Issues in Crime and Criminal Justice No. 400, Canberra: Australian Institute of Criminology, pp. 381-400, October 2010