Study of Cloud Security Problems

Zahra Jabeen[1], Mr. Mohd. Suaib[2]

[1]Integral University,
Kursi Road, Lucknow

[2]Integral University,
Kursi Road, Lucknow.

Abstract: *Cloud computing is the art of using a network of remote servers hosted on internet to save, process and manage data on demand and pay per use. Access to a pool of shared resources is provided instead of personal computers or local servers. As it does not acquire the things physically, it reduces managing cost and time for organizations. Research studies reveal that Cloud environment needs to recognize the importance of security within its various areas. There should be a bond of trust and privacy between the service provider and the client. Security must be viewed as a continuous process to meet the changing needs of a highly volatile computing environment. There is a need to have a holistic approach regarding cloud computing security methodology, which can be used in general, in any service model, at any stage till the client is using the service. There should be self-awareness from the client side too, regarding its own security. Keeping in view these observations, this study provided a detailed review of the existing literature and offered a number of research areas where future work is required, based on the existing published work.*

Keywords: *cloud, attacks, threats, multi-tenancy, security, problems, issues.*

1. Introduction

Cloud Computing is a distributed framework that centralizes resources of server on an extensible platform so as to provide on demand computing resources and services. Cloud Service Providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like Internet Service Providers (ISP's) offer costumers fast speed broadband for internet access. ISPs and CSPs both offer services.

Security processes that were once visible are now concealed behind levels of abstraction. This lack of visibility creates a number of Cloud Security issues. The focus is to identify issues in Cloud computing, which considers vulnerabilities, threats, attacks and their countermeasures to provide security at each layer of Cloud computing. These issues along with others have been looked into and various countermeasures have been provided but Cloud needs to be more secure and robust to fulfil the daily needs of the clients. There is a need for development of a process that would help to analyse all high/medium/low risks and provide countermeasures for the same.

A flexible model is provided by cloud for simplified remote access, IT management, mobility, remote access and cost-efficiency. Data privacy and software security are growing concerns as more mission-critical applications migrate to the cloud. [2]

2. Cloud computing architecture

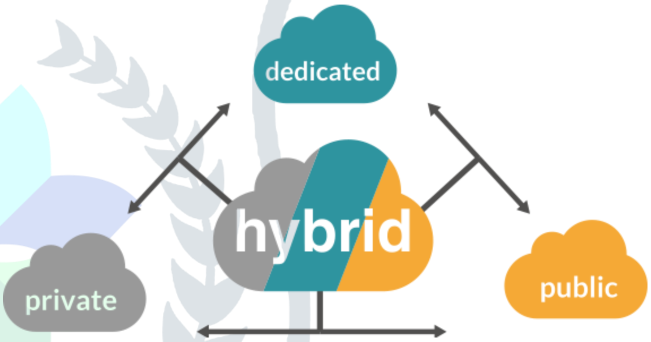

Figure 1: Cloud Deployment Models

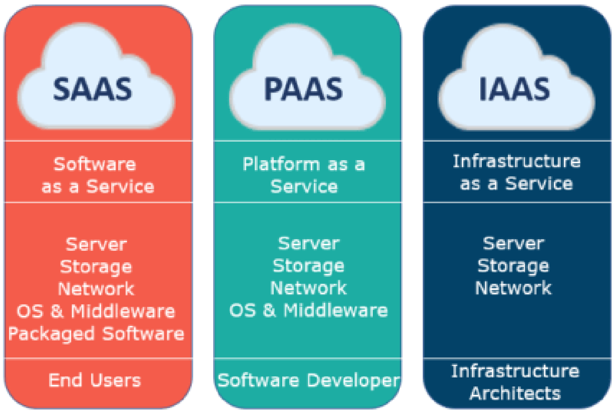

Figure 2: Cloud Service Models

3. Ten Critical cloud security threats in 2018

1. **Data breaches**
   A data breach risk is not unique to cloud computing, but it has consistently ranked as a top concern for cloud customers.

2. **Human error**
   According to Jay Heiser, research vice president at Gartner, "Through 2020, 95% of cloud security failures will be the customer's fault."[3]
3. **Data loss with no backup**
   A permanent loss of customer data can be leaded due to an accident or catastrophe if there are no measures in place to back up that data.
4. **Insider threats**
   A recent research report says, "53% of organizations surveyed have confirmed insider attacks against their organization."
5. **DDoS attacks**
   Cloud customers and providers pose significant risks due to distributed denial-of-service attacks including reputational damage, lengthy service outages and exposure of customer data.
6. **Insecure APIs**
   An API behaves as the public "front door" to your application is likely to be the initial entry point for attackers. Pen testing should be used to uncover security weaknesses in the APIs.
7. **Exploits**
   Shared memory and resources may create new attack surfaces for malicious actors because of multi-tenancy nature of the cloud (where customers share computing resources).
8. **Account hijacking**
   Attackers may gain access to critical areas of cloud computing services using stolen credentials, compromising the integrity, confidentiality and availability of those services.
9. **Advanced persistent threats**
   Most of the advanced persistent threat groups target cloud environments to conduct their attacks and also use public cloud services.
10. **Spectre & Meltdown**
    To view data on virtual servers hosted on the same hardware attackers can exploit Meltdown, possibly disastrous for cloud computing hosts. Spectre is however harder to exploit, but also harder to fix.

4. Research Challenges

Research on cloud computing addresses the challenges of meeting the requirements of next generation public, private and hybrid cloud computing architectures and also the challenges of allowing development and applications platforms to take advantage of the benefits of cloud computing.

Most of the existing issues have not been fully addressed, while new challenges keep emerging from applications. Some of the research challenging issues in cloud computing are given below:

• **Service Level Agreements (SLA's)** Most of the cloud vendors create SLA's to make a defensive shield against legal action while offering assurances to customers. So there are some issues such as data protection, outages and price structures that must be taken into account by the customers before signing a contract with the vendor.

• **Cloud Data Management** As service vendors don't have access to the physical security system of data centres, to achieve full data security they must rely on the infrastructure provider. In a virtual environment like the clouds, VMs can dynamically migrate from one location to another; hence using remote attestation directly is not enough.

• **Interoperability** Ability of a computer system to run applications from various vendors and to interact with other computers across LAN or WAN independent of their operating systems and physical architecture.

• **Multi-Tenancy** Multi-tenancy occurs when multiple consumers uses the same cloud, same operating system, on the same hardware, with the same data-storage system to share the information and data or runs on a single server. [1]

5. Conclusion

Research studies reveal that Cloud environment needs to recognize the importance of security within its various areas. There should be a bond of trust and privacy between the service provider and the client. Security must be viewed as a continuous process to meet the changing needs of a highly volatile computing environment. There is a need to have a holistic approach regarding cloud computing security methodology, which can be used in general, in any service model, at any stage till the client is using the service. There should be self-awareness from the client side too, regarding its own security.

Security issues cannot let us ignore the endless possibilities of cloud computing - the unending analysis and research for regular, robust and integrated security models for cloud computing may be the only way of inspiration.

We believe that due to the complication of the cloud, it might be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques are needed to be radically tweaked to be able to work with the clouds architecture. We hope our work will provide a better understanding of the design challenges of cloud computing, and pave the path for further research in this area.

6. References

1. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4,April 2018, ISSN: 2278 – 1323

2. International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN 2249-6831Vol. 3, Issue 3, Aug 2013, 305-314

3. https://www.synopsys.com/blogs/software-security/10-cloud-security-threats-2018/

4. Varsha et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June-2015, pg. 230-234

Author Profile

Zahra Jabeen received the BTech. degree in Co mputer Science Engineering from Bansal Institute of Engg & Technology in 2016. She is currently persuing her Mtech in CSE from Integral University, Lucknow.

Mr. Mohd. Suaib is currently assisstant professor at Integral university in cse department