STUDY ON SECURITY CORE ISSUES AND CHALLENGES IN CLOUD COMPUTING

Dr. A. Anthony Raj
Associate Professor,
Dept of CSE, PRIST University
Thanjavur 613403. Tamilnadu, India.

Abstract: According to a Forbes' study published in 2015, cloud-based security spending is expected to increase by 42%. To another research, the IT security expenditure had increased to 79.1% by 2015, showing an increase of more than 10% each year. International Data Corporation (IDC) in 2011 showed that 74.6% of enterprise customers ranked security as a major challenge. [1] The objective of our research is to understand the cloud computing advantages and its components, security issues, and risks, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud.
In this paper we think about the big picture of cloud computing security - extending across the potential issues and vulnerabilities associated with software platform; virtualization infrastructure; identity focus and access control; confidentiality and privacy; data integrity; physical and process security views; and legal compliance in cloud. We introduce our conclusions from the considering a matter of a cloud service provider, cloud consumer, and third-party authorities such as Govt. We also deal the threat models and their significance in cloud security in areas such as Information Centric Security, Privacy Preserving Models and Trusted Computing.

Index Terms **- Cloud computing, Security, Threat model, Vulnerabilities, Threats, Cloud Architecture.**

I. INTRODUCTION

According to Sharma and Trivedi, cloud computing is a set of resources that can scale up and down on-demand. It is available over the Internet in a self-service model with little to no interaction required with the service provider. Cloud enables new ways of offering products and services with innovative, technical, and pricing opportunities.[1]
According to Avram, there are some unique advantages to cloud computing. Some of the key advantages are:

- Cost of entry for all organizations including small firms
- Almost immediate access to the resources
- Reduction in IT barriers to innovation
- Easy to scale the services
- Implement and/or offer new class of application and delivery services

Before we dive into the security issues, it is important to understand the cloud architecture.

II. CLOUD ARCHITECTURE

As per NIST's Cloud Computing Reference Architecture, there are five major actors that influence and are impacted by cloud computing, along with its security implications. This paper focuses on cloud consumer and cloud provider's threat and risk perceptions.

Cloud Consumer A person or Organization that maintains a business relationship with, and uses service from, Cloud Provider

Cloud Provider A person, organization, or entity responsible for making a service available to interested parties

Cloud Auditor A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation

Cloud Broker An Entity that manages the use, performance, and delivery of cloud services and negotiates relationship between *Cloud providers* and *Cloud Consumers*

Cloud Carrier An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers* [1],[3]

It is important to note that the figure represents an end-to-end reference architecture that addresses all the seven layers of the Open Systems Interconnection (OSI) model, and extends to include the business, commercial, and governance aspects. As it is evident, cloud computing is a comprehensive and complex solution with many areas of vulnerabilities. [1]

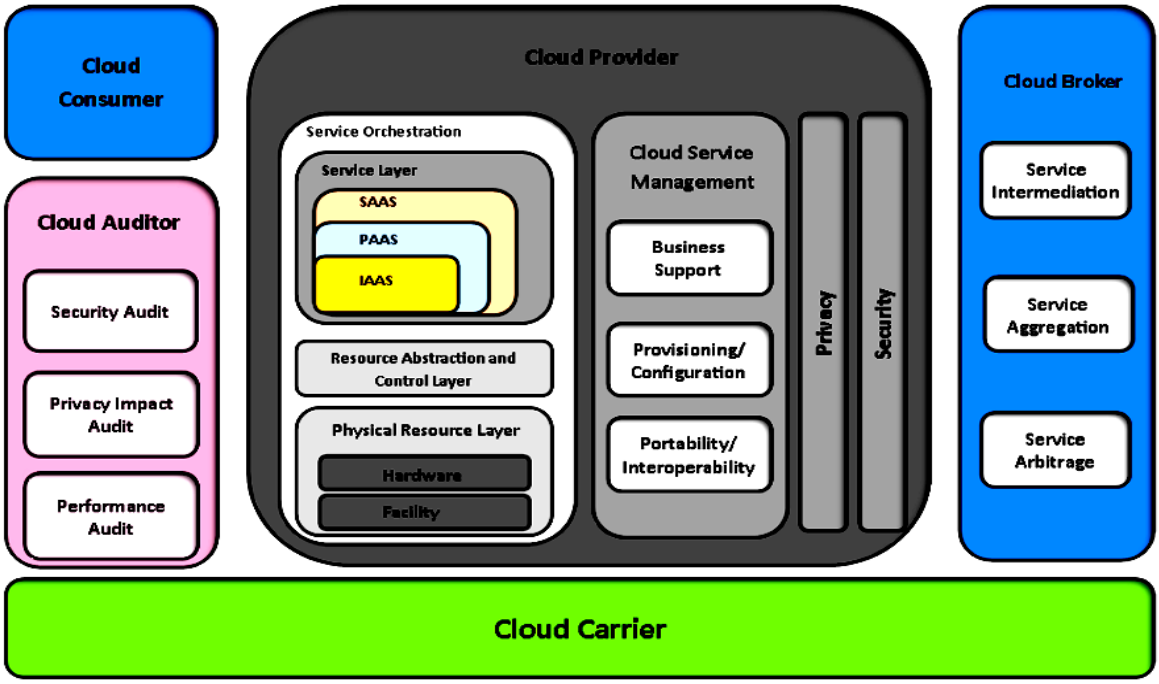

Figure1: Reference architecture for cloud computing.

I. THREAT MODEL

A threat model is one which helps in analyze the security level in a system suppose I am saying that I am going to protect the system from attack then what are the types of the attacks need to be enumerated so the threat model attempts to enumerate the different ways by which your system could be attacked. Threat model also plays a way for you to come out with mitigation strategies if I want to go and prevent an attack as such you should know the what the attack is, and then based on what the attack could be, I could now give a mitigation strategy and once I propose a mitigation strategy we can go and find out how effective would be in that context. A threat model helps us in Analyzing a security problem, Design mitigation strategies, and to evaluate solutions.

Table 1: Threat model steps

THERAT MODEL	
1.	Identify Attackers, Assets, threats, and other Components
2.	Rank the threats
3.	Choose Mitigation Strategies
4.	Build solutions based on strategies

So as we mentioned the steps listed above first we identify who can be the attackers? What on all the assets they could attack? First we identify the assets, what are the types of attacks for each attackers do on those assets? And then we go and rank the threats. Which are highly sensitive may be stealing of password may be highly sensitive threat, then we choose mitigation strategy in terms of this priority then we will build the solution based on the strategy. So this is a clear procedure for how to model the threat and come out with solution for the type. [2,4]

In our Context we are looking at our cloud and we will be looking the threat models for the cloud. Now basic components of the threat model would be how do you model an attacker? How do you list his goals? Based on this what are all the possible vulnerable threats to your system face? So your attacker can be inside your system or it can be outside the system, inside the system means those who have close access your physical system or part of your area network.

II. SECURITY IMPLICATION BASED ON DEPLOYMENT AND DELIVERY MODEL

The two most important aspects that determine the level of vulnerability in a cloud-computing platform is the choice of deployment and delivery model. According to Modi et al. & NIST4, there are three deployment and three delivery models that are considered as industry standards. Each of these three deployment and delivery models have unique security implications. The following sub-sections briefly discuss each of these models and their security implications: [1,5]

A. Cloud Deployment Model

The three most common types of cloud deployment models are

- Private Cloud
- Public Cloud
- Hybrid Cloud

TYPE I

Private Cloud

In a private cloud, the cloud service provider pools together scalable resources and virtual applications and makes them available to the cloud consumers. In this deployment model, the resources are dedicated to a single or a set of organizations and treated as intranet functionality. The billing usually is on a subscription basis with a cloud consumer making minimum commitments.

Implications

Positive security implications are relatively high and the organization has significant influence on the architecture, processes, and tools used in the deployment.

Challenges

Security challenges include high cost of implementation and management, skills requirement, and vulnerability management. In this deployment model, cost and return on investment are key factors and the security implementation is usually based on risk assessment and hence, the security cover is not comprehensive. [5][1]

TYPE II

Public Cloud

In a public cloud, resources are dynamically committed on a fine-grained, self-service basis over the Internet or a portal. Billing is usually consumption-based and is charged on a pay per use basis.

Implications

Positive security implications are that due to a large number of cloud consumers and volumes of transactions involved. The cloud service provider normally has a comprehensive & layered security system, which can potentially provide a high degree of security due to its implement once and use multiple times model, which significantly reduces the cost of security implementation for the consumer.

Challenges

Security challenges are heightened, as the resources are not committed but leveraged across multiple cloud consumers. This not only adds additional burden of ensuring all applications and data accessed on the public cloud, but also has to manage the multitude of external influences such as legislative, data protection etc.[1]

TYPE III

Hybrid Cloud

Hybrid cloud is a deployment model where a private cloud is linked to one or more external cloud services while being managed centrally. It provides the cloud consumers a flexible and fit-for-purpose solution with a relative ease of operations. The hybrid clouds have a higher degree of complexity in terms of billing and commercials.

Implications

Positive security implications are that security can be purpose-built for vulnerabilities, threats, and risks that are assessed. This makes it cost-effective and targeted.

Challenges

Security challenges are relatively high as the deployment model is complex with heterogeneous environment, multiple orchestration, and automation tools. This will require additional administrative overhead, with any oversight resulting in significant risk exposure.

B. Cloud Delivery Model

The three cloud delivery models proposed by NIST and adapted by the industry are

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Delivery Type A - Infrastructure as a Service (IaaS)

Description

Infrastructure as a Service is a multi-tenant cloud layer where the cloud service provider dedicated resources are only shared with contracted clients at a pay-per-use fee. This typically means that Operating System is presented to the cloud consumer. The cloud service provider's responsibility ends with the operating system.

Risk and responsibility

This is a great model where the cloud consumer builds the application without worrying about the infrastructure requirements. The security responsibility is equally divided between the cloud service provider and the cloud consumer. In this model, the risk is segregated and layered. It is also a shared risk model. [1]

Delivery Type B -Platform as a Service (PaaS)

Description

Platform as a Service is one of the more popular delivery services where the cloud provider provisions not just the operating system but also a development stack. It is a common practice for providers in this model to provide database and application administration along with development services. Just as in IaaS, PaaS is a pay-per-use model.

Risk and responsibility

This is an appropriate model, where the cloud consumer brings the application expertise along with licenses, data, and resources, and consumes the platform shell. This model is used by consumers who either lack infrastructure skills or want to save on high capital expenditure (capex) spend required to build the infrastructure. In this delivery model, the security responsibility starts to tilt more towards the cloud provider. Similar to IaaS, this is a shared risk model; however, the service provider bears higher risk than consumer as the provider supports more layers. [1],[6]

Delivery Type C - Software as a Service (SaaS)

Description

In a Software as a Service model, the complete application stack is hosted by the cloud provider, who provides end-to-end resources, including licensing, application, networking etc., The cloud consumer, typically brings the data and business processes to consumes the services in a web service or software-oriented architecture.

Risk and responsibility

This model is very effective in cases where the cloud consumer does not have the necessary skills, time, or resources to setup an application ecosystem and manage it. This model also provides the best commercial benefit with no upfront capex requirement. The security responsibility is mostly with the cloud provider. The consumer is mainly responsible for securing the client-side vulnerabilities. In this model, the service provider bears most Risk [3][1]

III. CORE ISSUES

Now the core issue in this stuff is the lack of trust and the other thing is that why there is a lack of trust? And why there is going to be problem because lack of trust? We need to see that everything in detail.

What is the issue?

- The core issue is level of Trust
- Many cloud computing providers trust their customers
- Only the outsider is evil and not the customer
- Logical isolation but physical sharing of resources
- But what if those inside are also evil.

Important network level issue is access control somebody wants to access the cloud outside then we need to have strong authentication mechanism and authorization. Once we authenticate and authorize them to use the control resources and then both the authentication and the authorization is to be audited. This should be done all the resources allocated in the curve. So authorization, Authentication and auditing of what the user is doing can be done at the network level. [5,6]

This emergent cloud technology is facing many technological challenges in different aspects of data & information handling & storage.

Some of the challenges are as follows:

- Interoperability
- Performance
- Portability
- Availability & reliability
- Security & Privacy[4,6]

IV. CONCLUSION

Cloud computing is a model that helps to speed up and increase the flexibility of data management with reduced cost. It is undeniable that cloud computing has brings us lots of benefits and becoming more popular nowadays. Many large companies start using cloud service in their business. While the cloud computing is widely used, the security becomes a concern to everyone who use cloud services. There is a lot of security arises continuously while there are improvement as well on the security model of the cloud service provided. Despite the increasing use of the cloud service, the user should use the cloud service provided wisely in a way that always ensure good security practices so that this technology have the potential to bring the information technology to the next level. Cloud computing might help us to separate the software from the hardware as more technologies are used as service using cloud and software might have a highly abstract space with the computer hardware. It is expected that this paper provides some basis or foundation in regards to issues and challenges in cloud computing.

REFERENCE

[1]. Gururaj Ramachandra , Mohsin Iftikhar "A Comprehensive Survey on Security in Cloud Computing" in 3rd International Workshop on Cyber Security and Digital Investigation: ScienceDirect Procedia Computer Science 110(2017)465-472
[2]. Shubhashis Sengupta, Vikrant Kaulgud "Cloud Computing Security – Trends and Research Directions." Accenture Technology Labs, No.4/1,IBC Knowledge Park,Bannerghatta Road,Bangalore 560029.
[3]. Y Z An, Z F Zaaba & N F Samsudin "Reviews on Security Issues and Challenges in Cloud Computing" School of Computer Sciences, Universiti Sains Malaysia, 11800 Minden,Pulau Pinang,Malaysia.
[4]. Nelson Gonzalez, Charles Miers "A quantitative analysis of current security concerns and solutions for cloud computing." In Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012,1:11 A SpringerOpen Journal.
[5]. Keiko Hashizume, David G Rosado "An analysis of security issues for Cloud computing" in Hashizume et al. Journal of Internet of Services and Applications 2013,4:5
[6]. N. Pradheep, M. Venkatachalam, M. Saroja, S. Prakasam "Privacy and Security Issues in Cloud Computing Using DaaS Models." In Department of Electronics, Erode Arts and Science College (Autonomous), Erode – 638009.