LAYERS BASED SECURITY ISSUES IN CLOUD COMPUTING

John Jeya Singh.T[1], Dr E.Baburaj[2]

[1] *Research Scholar, Reasearch and Development Center.,Bharathiar University, Coimbatore ,Tamilnadu, (India).*

[2] *Professor and Head, Dept of Computer Science & Engineering, Narayanaguru College of Engineering, Majalumoodu, Tamilnadu, (India)*

ABSTRACT

Cloud computing is generally recognized as a technology which will have a significant impact on IT in the future. Cloud computing can offer a verity of services (Like networks, servers, Storage, application etc,) through the internet. Resources are available to the cloud. So we can access from cloud at any time and any location via the internet. In this paper we summarize Cloud computing Layer based security issues .We have suggested feasible and available solutions for the same.

Keywords: Cloud Computing, Layered Model, Physical Layer, Infrastructure Layer, Platform Layer, Application Layer

I. INTRODUCTION

Cloud computing is a new Computing Technology in the present day scenario with almost all the organizations trying to make an entry into it. Cloud can be viewed as a pool of resources where service providers provide services to users through internet. The main advantages of cloud computing are cost saving, high availability and easy scalability [1].There are three common services provided by cloud [2] Software as a Service (SaaS), Platform as a Service (PaaS), and infrastructure as a service (IaaS).This Cloud modal offers four types of deployment models is Private Cloud, Community cloud, Public Cloud and Hybrid Cloud.

In this paper, we discuss cloud computing, its types and cloud computing services. The remainder of this paper is organized as follows. Section 2 described Cloud computing layered model. Section 3 described Layers based security threats Section 4 we given suggested feasible and available solution. Section 5 will conclude the paper.

II. CLOUD COMPUTING LAYERED MODEL

In this section we describe cloud computing layers.

The architecture of cloud computing environment can be divided into four layers (fig 1). They are Application Layer, Platform Layer, Infrastructure Layer and Physical Layer.

Fig 1.Cloud Computing Layer Model

2.1 Physical Layer

The Physical layer, is lowest layer in the stack. This layer is typically implemented in data centers. This layer is responsible for managing all physical resources like servers, routers, switches, power and cooling systems. The physical layer is sometimes referred to as the server layer or hardware layer.

The provider can use software to monitor the connection topology, memory use, bus speeds, processor loads, disk storage, temperature, voltage and so on. The customer can be interacts only virtualized environment.

2.2 Infrastructure Layer

The infrastructure layer also called as virtualization layer. At this layer, you would need to have full access and control over your infrastructure in order to set up active Directory and other protocols. Virtual machine technology is commonly used in this layer. It provides software abstraction. Cloud customer can interact directly with virtual layer.

This Layer consists of multiple sub layers, Virtual Machine (VM), Virtual Network and Virtual Storage. There are many major players in this commodity layer such as VMware, Citrix, Sun Microsystems and Microsoft.

2.3 Platform Layer

The Platform Layer also called as middleware Layer. The platform layer consists of an operating system and application frameworks. This layer to provide API support for implementing storage, database and business logic of typical web applications. E.g. Google App Engine(Python framework) and Force.com(Programming language called Apex).

In this layer customers can create an application within an existing API or programming language. The examples of Cloud products include Google App Engine, Microsoft Azure and so on. Google App Engine has provided two platforms of Python and Java. While Microsoft Azure provides a variety of different programming tool platforms [3].

2.4 Application Layer

The application layer can also be called SaaS interface layer. The application functionality is served via the internet (eg Gmail,CRM). This layer is most important and utilized layer and closed with end user of cloud computing. This layer must be well aware of Java script, XML and Perl languages, back end infrastructure applications like Apache, Tomcat and SQL[4].

The application layer subdivided into three layers. The model consists of a presentation layer, Business layer and data layer. The presentation layer describes the application user interactions, the business layer describes the business logic and the data layer is used for application data storage. The data layer is subdivided into the Data Access Layer (DAL) and Database Layer (DBL).The DAL encapsulates the data access functionality, DBL is responsible for data persistence and data manipulation.

III. LAYER BASED SECURITY THREATS

Security issues could be classified into two. First one Access Security, Secondly Service Security. Access Security Communications to the cloud service provider is a potential point at which threats to the service could be exposed. Service Security, most of the security threats are possible at the point of service provision and this could include the actual device security at the cloud provider and the storage security used by the provider. The

service providers, they would be able to provide robust security with the use of firewalls and malware protection.

3.1 Physical Layer Security Threats

In this section we describe important Physical Layer Security Threats.

3.1.1 Line and Clocking Problems

Clocking problems with serial connections can lead to either chronic loss of the connection or to degraded performance [5].

3.1.2 Operating Expense

The high cost associated with physical layer maintenance has a direct impact on operating expenses. Accurate knowledge of physical layer topology leads to less network issues and faster resolution of problems.

3.1.3 Capacity and Scale

The ever increasing amount of data and number of devices on the network continues to drive complexity in the physical layer.

3.1.4 Compliance

There are a variety of government regulations, compliance and reporting requirements regarding how an organization's data are accessed, transacted and stored. Existing network management tools do not enable intrusion detection and logging of events as related to physical layer connections.

3.1.5 Traffic shaping

Traffic shaping, also known as packet shaping, Quality of Service (QoS) or bandwidth management, is the manipulation and prioritization of network traffic to reduce the impact of heavy users or machines from affecting other users. This bandwidth throttling or rate limiting is performed to guarantee QoS and return on investment (ROI) via the efficient use of bandwidth [6].

3.1.6 Bandwidth

Physical layer is not capable of handling the vast bandwidth that true cloud computing [7].

3.1.7 Cooling

Data center cooling is becoming a hot topic. In fact, as agencies load up on big data and move to the cloud, more data centers will be coming online, and cooling may become one of the biggest problems.

3.2 Infrastructure Layer Security Threats

In this section we describe important Infrastructure Layer Security Threats.

3.2.1 Service Level Agreement (SLA)

A Service Level Agreement (SLA) is a part of a service contract between the consumer and the provider that formally defines the level of service. The main goal of establishing SLA process is to improve the Quality of Experience of the service or product to the enterprise customer and reach the satisfaction level.

In Cloud computing, SLAs are obligatory to control the use of computing resources. Therefore, a main issue for Cloud computing is to build a new layer to maintain a negotiation phase between service providers and consumers to establish SLAs between them.

3.2.2 Virtualization

Virtualization provides many features to the users to create, share, migrate, copy, rollback virtual machines which helps in running many applications on them [8, 9].

Hypervisor can steal the data from the virtual machines. Hypervisor also called as virtual machine manager is a program to share a single hardware host of multiple operating systems. It controls the host processor and resources, takes care the allocation of resources to operating systems. There are two types of attacks that are occurring on hypervisor [10] attack on hypervisor through the host Operating System(OS) and attacks on hypervisor through a guest OS.

3.2.3 IP spoofing

A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host [11].

3.2.4 Port Scanning

Port Scanning is the name for the technique used to identify open ports and services available on a network host. It is sometimes utilized by security technicians to audit computers for vulnerabilities however, it is also used by hackers to target victims. It can be used to send requests to connect to the targeted computers, and then keep track of the ports which appear to be opened, or those that respond to the request.

3.2.5 Man-in-the-middle attack

An attack where a user gets between the sender and receiver of information and sniffs any information being sent. In some cases, users may be sending unencrypted data, which means the man-in-the-middle (MITM) can obtain any unencrypted information. In other cases, a user may be able to obtain information from the attack, but has to unencrypted the information before it can be read [12].

3.3 Platform Layer Security Threats

In this section we describe important Platform Layer Security Threats.

3.3.1 Technical Immaturity

Every cloud framework has its own interface methods, services and costs. The unfolding nature of the platform-as-a-service approach puts everything at risk costs could change overnight, services could be dropped, and quality of service could worsen. Standards bodies are just beginning to look at the market [13].

3.3.2 Underlying Infrastructure security

Cloud providers are responsible for the underlying infrastructure security and the services running for applications [14]. So, the application developers have no privilege to access underlying infrastructure.

3.3.3 Application development life cycle

It is also a big challenge to secure a software application development because software developers face quite difficult to secure the application taking place in the cloud environment. The application needs to be upgraded by applying new patches or versions to keep them up-to-date and secure [15].

3.3.4 Vendor lock-in

Because cloud computing is still relatively new, standards are still being developed. Many cloud platforms and services are proprietary, meaning that they are build on the specific standards, tools and protocols developed by a particular vendor for its particular cloud offering. This can make migrating off a proprietary cloud platform prohibitively complicated and expensive. Three types of vendor lock-in can occur with cloud computing [16].

3.4 Application Layer Security Threats

In this section we describe important Application Layer Security Threats.

3.4.1 Insecure Interfaces and APIs

Cloud computing provides number of interfaces and APIs to interact with the services provided to the user organizations and third parties. It is often built upon these interfaces to offer value added services to their customers. This introduces the complexity of the new layered API, it also increases risk, as the organizations may be required to relinquish their credentials to third parties in order to enable their agency [17].

3.4.2 Denial of service attacks

The biggest security threat to the Cloud is an application layer distributed denial of service (DDoS) attacks. Hackers have found and are actively exploiting weaknesses in Cloud defenses, utilizing cheap, easily accessible tools to launch application layer attacks. A major reason they have been successful is that enterprise data centers and Cloud operators are not well prepared to defend against them. The DDoS attack is an attempt to make the service unable to use, which is assigned to the authorized users [18].

3.4.3 Dictionary Attack

In this attack attacker makes a file with some group of words which is probable by the user to set the password.

3.4.4 Buffer Overflow Attack

A buffer overflow attack is when the attacker sends more data to an application than is expected. A attacker gaining administrative access to the system in a command prompt or shell.

3.4.5 Account or Service Hijacking

Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites.

3.4.6 Data Loss

Cloud computing service providers handling high volumes of data, it's almost inevitable that some data loss will occur. This could be especially damaging if the client is relaying sensitive (not easy to recover) information over your cloud computing services network. In the summer of 2012, attacker broke into Mat's Apple, Gmail and Twitter accounts [19]. Through that access they erased personal data of the clients of those providers. The cloud lost data due to that reasons other than malicious attackers.

IV. PROPOSED SOLUTIONS TO ENHANCE CLOUD DATA STORAGE

There are several groups working and interested in developing standards and security for clouds. The Cloud Standards website is collecting and coordinating information about cloud related standards under development by other groups. The Cloud Security Alliance (CSA) is one of them [20]. CSA gathers solution providers, non profits and individuals to enter into a discussion about the current and future best practices for information assurance in the cloud.

4.1 Physical layer Issues solution

- Data encryption before storing it at virtual location, encrypt the data with your own keys and make sure that a vendor is ready for security certifications and external audits [21].
  Reporting of security incidents, personnel and physical layer management should be evaluated .
- CSP should maximize the user control and provide feedback [21].

- Organizations need to run applications and data transfer in their own private cloud and then transmute it into the public cloud.

4.2 Infrastructure Layer Issues Solution

- Use encryption for sending out private information online [22].
- Make use of an access control list (ACL) to block private or unauthorized IP addresses [22].
- Configure your Internet router to automatically reject unauthorized users on your local network.
- If possible, you should scan all 65,534 TCP ports on each network host that your scanner finds [22].
- Download the latest version of high security Web browsers such as Internet Explorer 7 or higher, Firefox 3 or higher, Google Chrome, Safari or Opera.
- Firewall protects resources from attacks.
- IDS/IPS(Interruption Detection System and Intrusion Prevention System) provides flexible defensive strategies to protect systems.

4.3 Platform Layer Issues Solution

- The provider is responsible to protect the integrity and privacy of the user object.
- Cryptographic methods help sensing the modifications or hiding the content.
- Signatures can be used to detect modifications.

4.4 Application Layer Issues solution

- Strong key generation, storage and management and destruction practices should be implemented.
- Provider backup and retention strategies should be specified contractually.
- Cloud provider security policies and SLAs should be understood clearly.
- Data backup should be carried out at regular intervals.
- Install trusted Antivirus and spyware Antivirus and Updates must be done without fail.
- Never download on the unknown antispyware program never be downloaded.
- Freeware downloads must be avoided [24].
- Buy and use intrusion detection system.
- Regulate device description downloads based on Router Hops [25].

V. CONCLUSION

The past few years cloud computing become very popular in the promising and competitive business world. It is one of the fastest growing fields in the IT industry. Cloud computing is revolutionizing how information technology resources and services are used and managed, but new revelation always comes with new problems. In this paper we have discussed various Layer security risks in Cloud Computing and also suggested solution for the same.

REFERENCES

[1] R.Maggiani. Communication Consultant, Solaris Communication,"*Cloud Computing is Changing How we Com*municate",2009, IEEE International Professional Conference, pp 1-4.

[2] M.Armbrust el al., "*A View of Cloud Computing*", Communications of the ACM,Vol 53,no 4.pp 50-58,2010.

[3] Available from http://blog.gogrid.com/2009/03/26/navigating-the-layers-of-the-cloud-computing-pyramid/#sthash.9i8TMh5A.dput

[4] Available from http://talkcloudcomputing.com/cloud-computing-four-layers-and-the-required-skill-set.

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

[6] Available from http://www.a10networks.com/glossary/traffic_shaping.php

[7] Zaigham Mahmood, Richard Hill, "*Cloud Computing for Enterprise Architectures (Google eBook)*",Springer Science & Business Media, 01-Dec-2011 - Computers,pp 58.

[8]. Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35–41.

[9]. Garfinkel T, Rosenblum M (2005) When virtual is harder than real: Security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa.

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

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

[12] Available from http://www.computerhope.com/jargon/m/mitma.htm

[13] InformationWeekanalytics.com,Dr.dobb`s Cloud computing: Platform as a service.

[14]. Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16 (3):23–25.

[15]. Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36–42.

[16] Hinkle,Mark.(2010-6-9)"Threecloud lock-in considerations", Zenoss Blog.

[17] CSA (Cloud Security Alliance), "*Top threats to cloud computing 2013*", pp 1-21, February 2013.

[18] Software Engineering Institute Carnegie Mellon, denial of service attacks. www.cert.org/tech_tips/denial_of_service.html.

[19] MAT HONAN, "*Hacked: Passwords have failed and* it's *time for something new*", 17 JANUARY 13.

[20] Available from https://cloudsecurityalliance.org.

[21] Jianfeng Yang and Zhibin Chen, Cloud Computing Research and Security Issues, 2010 IEEE 978-1-4244-5392-4/10, 2010.

[22] Available from http://www.ehow.com/how_6869712_avoid-ip-spoofing.html.

[23] Available from http://www.dummies.com/how-to/content/prevent-network-hacking-with-port-scanners.html.

[24] Tips to stop or Reduce Threats Posted by DDoS,9/14/2011 http://brighthub.com/computing/enterprise-security/articles/106930.aspx.

[25] Available from http://support.microsoft.com/kb/315056.aspx.