Bottle-Necks of Cloud Security- A Survey

Soumya Ranjan Jena
Teaching Associate
Department of CSA
AKS University, Satna, M.P, India

ABSTRACT

A tremendous necessity has enlarged its domain in security in cloud computing. This paper is a survey more specific to different security issues that are raised in cloud computing environment. However, cloud computing is one of the recent research immersing trends for hosting and delivering services over the internet. It provides software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) to the end users. Cloud Computing enables ubiquitous, 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. It also provides scalability for applications by providing virtualized resources dynamically. Apart from these features cloud computing has several security challenges like storage security, data security, network security and application security.

General Terms

Cloud Computing, Cloud Security

KEYWORDS

Secure cloud computing, Cloud security, SaaS security issues, PaaS security issues, IaaS security issues, Cloud threats, Third party security.

1. INTRODUCTION

The cloud computing is a distributed computing paradigm which facilitates the users with distributed access to scalable virtualized hardware or software [1]. In this service the critical need is to store, manage, share and analyze large amounts of data in order to be secure. The major security challenge with cloud is that the owner of the data may not have full-fledged control where the data is to be store. This is because if one wants to exploit the benefits of cloud computing, then he must also have to utilize the resource allocation and scheduling provided by cloud which can be public or private or hybrid. Therefore we need to take utmost safeguard while transferring the data through untrusted processes.

2. CLOUD COMPUTING MODELS

According to NIST, cloud consists of three different service layers. Each layer has different functionalities and different services that are described as follows [2].

Software as a Service (SaaS): This service model provides different types of applications which are given by service provider on a cloud environment. Clients are able to access these applications with the help of interfaces like web browsers or application interfaces. Cloud application services or "Software as a Service (SaaS)" provide the function [2] of software as a service over internet. The customer does not need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except the some configuration setting for the application. Examples of Saas are Google Apps, Microsoft office live, Salesforce.com, Yahoo Zimbra etc.

Platform as a Service (PaaS): This service model facilitates the customer to deploy their application at the cloud environment with the use of programming and there is no need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except the some configuration settings for the application where it is going to host. It also provides all the facility without the purchasing, managing and other cost of software and hardware. Examples of Paas are Google's App Engine, Amazon's EC2 , Microsoft's Azure platform, Net Suite etc.

Infrastructure as a Service (IaaS): This service provides the consumer to provision processing, storage, networks, and other fundamental computing resources. In this kind of the service consumer is able to deploy and run arbitrary software, which can include operating systems and applications. Most popular services of IaaS today include Amazon, IBM Blue Cloud, Sun Project Caroline.

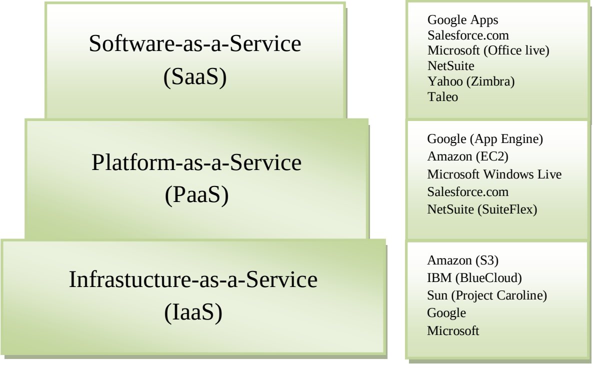

Fig 1: Architecture of cloud computing service layers

3. PROBLEM DEFINITION

Why security is the biggest threat in cloud computing? Security is the basic and primary requirement for any networking model like cloud based infrastructure. According to IDC [4] security ranked as the greatest challenge or issue attributed to cloud computing (Refer Fig: 2). Before analyzing security aspects in Cloud Computing, we need to understand the relationships among cloud service models [3]. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will hamper the security of both PaaS and SaaS services, but also it may be true on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a result of these deep dependencies, any attack to any cloud service layer can compromise the upper layers. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. These relationships and dependencies between cloud models may also be a source of security risks.

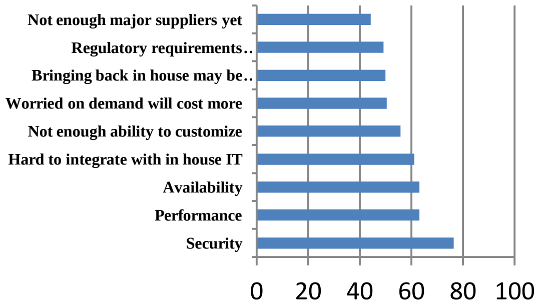

Fig 2: Rate of challenges/issues in cloud computing by IDC

4. SaaS SECURITY ISSUES

SaaS users get less protection in comparison to the users of other services of cloud computing. Therefore the users of SaaS face many security concerns in comparison to other services.

4.1 WEB BAED APPLICATIONS

Web based applications are generally delivered through the internet on a Web browser. However, flaws in these applications lead to vulnerabilities for SaaS. Attackers use the web to compromise user's computers and perform malicious activities that include stealing sensitive and confidential data. Security challenges in SaaS applications are very much similar to web based application technology, however the traditional security solutions aren't so much effective to protect it from attackers. Therefore, new techniques and advancements are essentially required.

4.2 ACCESSIBILITY

Now-a-days it is an easier task to access web based applications over the internet through web browser on any network devices like public computer and mobile device. Accessing web on a public computer increases the possibility of risk. In December 2009, Cloud Security Alliance [5] has released a document that narrates the current state of cloud computing and the top threats in this area such as information stealing, vulnerabilities, insecure marketplaces, and proximity-based hacking.

4.3 DATA SECURITY

In cloud computing the service and data maintenance is provided by the provider or vendor which leaves the client/customer unaware of where the processes are running or where the data is stored [. So, logically speaking, the client has no control over it. Since the cloud computing uses the internet as the communication media strong encryption with key management is essentially required to protect data. The SaaS provider is the one responsible for the security of the data while being processed and stored. Therefore, in SaaS organizational data is often processed in plaintext and stored in the cloud. Again, disaster recovery and data backup [6] are the key ingredients of data protection in SaaS applications. However, these introduce security concerns as well.

4.4 MULTI-TENANCY

Multi-tenancy in cloud service is a policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies [7]. In case of multi-tenancy each business customer get different security, service level agreements (SLA), governance, and chargeback policies on cloud based shared infrastructure. This infrastructure can be a virtualized private or public cloud as shown in Fig: 3 and 4.

In the case of a private cloud, a single organization may have a multitude of third party consultants and contractors, as well as a desire for a high degree of logical separation between business units. However, in case of public cloud a customer has only a third party consultant. Therefore, it is very much essential to impose security concerns in case of multi-tenancy.

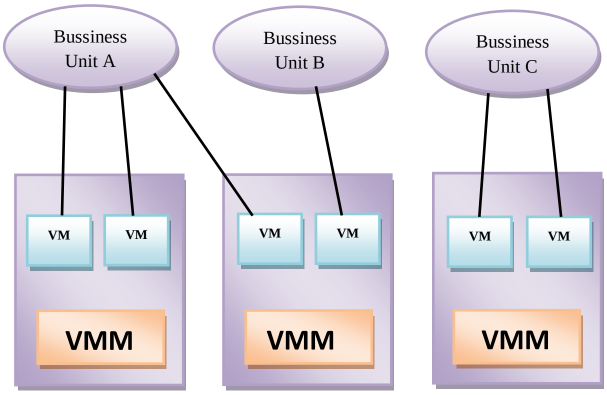

Fig 3: Multi-tenancy in virtualized private cloud

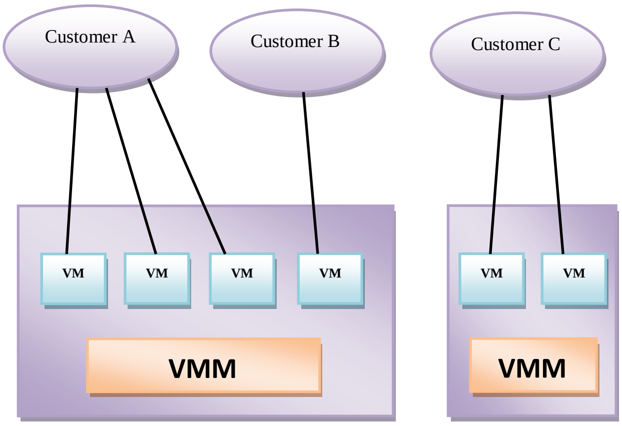

Fig 4: Multi-tenancy in virtualized public cloud

5. PaaS SECURITY ISSUES

PaaS model is based on the service-oriented architecture (SOA). Therefore the PaaS model inherits all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks, etc. So this security issue is a shared responsibility among cloud providers, service providers and consumers.

5.1 TRUSTED THIRD PARTY AUDITOR

Cloud computing provides storage of data at a remote site to maximize resource utilization. This brings the importance about data to be protected and only to be given to the authorized person. This essentially amounts to secure third party auditor of data that is necessary for ensuring security and integrity of data. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. The trusted third party can be relied upon for [8]:

- Low and high level confidentiality.
- Server and client authentication.

- Creation of security domains.
- Cryptographic separation of data.
- Certificate-based authorization.
- Access control framework

Moreover in secure third party auditor the owner of the document specifies access control policies for the documents to the publisher. When the subject requests a document, the publisher will apply the policies related to subjects and give portions of the documents to the subject. As the publisher is untrusted the owner of the document will encrypt various combinations of documents by using his private key.

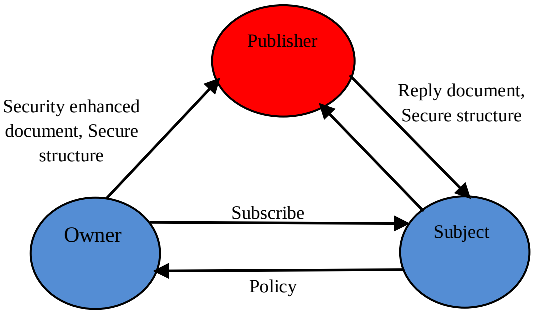
Publisher
Security enhanced document, Secure structure
Reply document, Secure structure
Owner
Subscribe
Subject
Policy

Fig 5: Secure third party audit

5.2 LIFE CYCLE DEVELOPMENT

It is an utmost challenge for developers to build secure applications that may be hosted on the cloud. Cloud computing affects all aspects of software development life cycle (SDLC) i.e. spanning application architecture, design, development, quality assurance, documentation, deployment, management, maintenance, and decommissioning. Developers -have to keep in mind that PaaS applications should be upgraded frequently, so they have to ensure that their application development processes are flexible enough to keep up with changes. Besides secure development techniques, developers need to be educated about data legal issues as well, so that data is not stored in inappropriate locations. Data may be stored on different places with different legal regimes that can compromise its privacy and security.

5.3 INFRASTRUCTURE SECURITY

In cloud computing always the lower layer provides facilities to upper layer. Therefore, PaaS offers development tools to create SaaS applications. Moreover, these two use multitenant architecture to facilitate multiple concurrent users to utilize the same software.

6. IaaS SECURITY ISSUES

IaaS provides computational and storage infrastructure in a centralized, location-transparent service over a virtualized systems which are accessed through the internet [2] [9]. It also provides the users to run any software with full control and management on the resources allocated to them. As virtual machine monitor are used in IaaS infrastructure so there is less security breaches takes place. But however there are some security aspects that are found in IaaS.

6.1 VIRTUALIZATION

Virtualization is the ability to provide multi-tenant cloud services at the infrastructure, platform, or software level is often underpinned by the ability to provide some form of virtualization to create economic scale [7]. Different virtualization technologies that provide virtualized environment are VMWARE, XEN, and KVM. Moreover, virtualized environments are vulnerable to all types of attacks for normal infrastructures; but security is a greater challenge since it has more interconnection complexity. Therefore, according to the Cloud Security Alliance [9] the following precautions we need to take for virtualization.

- We first need to understand what type of virtualization our cloud provider uses.
- Virtualized operating systems should be parameterized by third party security technology to support layered security controls and reduce dependency.
- We need to understand which security controls are in place internal or external to the VMs. Internal security protects intrusion detection, vulnerability, virus, etc. Whereas external securities to the VMs protect administrative interfaces such as web-based, APIs that exposed to the customers.
- We need to validate the pedigree and integrity of any VM image or template originating from the cloud provider before using.
- VMM (Virtual Machine Monitor) or hypervisor is solely responsible for virtual machines isolation; therefore we need to keep the virtual machine as simple as possible which will ultimately reduce the risk of security vulnerability.
- Administrative access and control of virtualized operating systems is crucial, and should include strong authentication.
- A virtual machine should be able to roll back to its previous state if an error happens.
- We should carry out secure mapping of virtual machines to physical machines.

7. THREATS IN CLOUD COMPUTING

Most of the important threats to cloud computing are [3][5]:

- **Service hijacking:** It is a type of account theft. Here an attacker gain access to user’s credential and can perform any type of malicious activities.
- **Data leakage:** It happens when data gets into the wrong hand.
- **Denial of service:** Here the system cannot satisfy any request from other legitimate users due to resources being unavailable.
- **VM escape:** It is designed to exploit the hypervisor in order to take control of the underlying infrastructure.
- **VM hopping:** In this case one VM is able to gain access another VM.
- **Malicious VM creation:** An attacker who creates a VM image containing malicious code such as Trojan horse and store it in the provider repository.
- **Sniffing/Spoofing:** A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs.

8. SECURITY THROUGH HDFS

HDFS stands for Hadoop Distributed File System which was first introduced by Apache. It is a superior software component for cloud computing environment that are used for secure query processing. It is based on master-slave approach [9][10]. Basically, Hadoop is a framework for running applications on large clusters built of commodity hardware [12].

An HDFS cluster consists of a single Name node as shown in Fig: 6. It has a master server that manages the file system namespace and regulates access to files by clients. In addition, there are a number of Data nodes, usually one per node in the cluster, which manages storage attached to the nodes that they run on. HDFS exposes a file system namespace and allows user data to be stored in files. Internally, a file is split into one or more blocks and these blocks are stored in a set of Data nodes. The Name node executes file system namespace operations like opening, closing, and renaming files and directories. It also determines the mapping of blocks to Data nodes. The Data nodes are responsible for serving read and write requests from the file system's clients. The Data nodes also perform block creation, deletion, and replication upon instruction from the Name node.

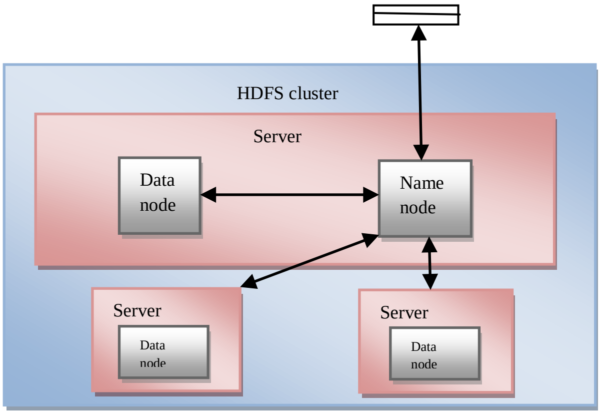

Fig 6: HDFS Architecture

9. MAPREDUCE FRAMEWORK

The MapReduce is a programming model [11] and an associated implementation for processing and generating large data sets across the Google's worldwide infrastructure. The MapReduce model performs two basic functions: Map() function that performs filtering and sorting (such as sorting students by first name into queues, one queue for each name) and a Reduce() function that performs a summary operation (such as counting the number of students in each queue, yielding name frequencies). The "MapReduce System"[11] (also called "infrastructure" or "framework") harmonizes by marshaling the distributed servers, running the various tasks in parallel, managing all communications and data transfers between the various parts of the system, and providing for redundancy and fault tolerance.

The model is inspired by map and reduce functions commonly used in functional programming, although their purpose in the MapReduce framework is not the same as in their original forms. Furthermore, the key contributions of the MapReduce framework are not the actual map and reduce functions, but the scalability and fault-tolerance achieved for a variety of applications by optimizing the execution engine once.

10. CONCLUSION & FUTURE WORK

Security is a greater challenge to every IT engineer for providing a reliable environment in cloud based infrastructure. Many of the security issues identified are observed in other computing environments: authentication, network security and legal requirements, for example, are not a novelty. However, the impact of such issues is intensified in cloud computing due to characteristics such as multi-tenancy and resource sharing, since actions from a single customer can affect all other users that inevitably share the same resources and interfaces. On the other hand, it is a new challenge to provide efficient and secure virtualization which allows multiple users to share a physical server.

A secure cloud computing environment depends on several security solutions working harmoniously together. By deploying a line of defense including firewall, intrusion detection and prevention, integrity monitoring, log inspection, and malware protection as software on virtual machines is the most effective method to maintain integrity of compliance and preserve security policy protection as virtual resources move from on-premise to public cloud environments.

11. ACKNOWLEDGEMENTS

For his timely and worthy inspiration, I am very much indebted to Er. Anant Kumar Soni, The Chairman, AKS University, Satna. I would also like to thank Dr. G.K.Pradhan, Dean of Engineering & Technology, AKS University, Satna. Last but not the least; I am thankful to Mr. Abhaya Kumar Jena for his help in preparation of the text.

12. REFERENCES

[1] Soumya Ranjan Jena and Zulfikhar Ahmad, "Response time minimization of different load balancing algorithms in cloud computing environment", IJCA, Volume-69, No-17, May 2013 edition.

[2] Sean Carlin, Kevin Curran, "Cloud computing technologies", IJ-CLOSER, Vol.1, No.2, June 2012, pp. 59-65, ISSN: 2089-3337.

[3] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing",Springer,Feb,2013.

[4] F. Gens, "New IDC IT Cloud Services Survey: Top Benefits and Challenges", *IDC eXchange*, Available: http://blogs.idc.com/ie/?p=730.

[5] Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho, Mats N¨aslund and Makan Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing", Springer, July,2012.

[6] B.R Kandukuri, V.R Paturi, A Rakshit, , "Cloud security issues", Services Computing, 2009. SCC '09. IEEE International Conference.

[7] Subashini S, Kavitha V , "A survey on Security issues in service delivery models of Cloud Computing", J Netw Comput Appl, 2011.

[8] Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues", Elsevier, 2010.

[9] Cloud Security Alliance, "Security guidance for critical areas of focus in Cloud Computing V3.0", 2011.

[10] Morsy MA, Grundy J, Müller I, "An analysis of the Cloud Computing Security problem", Proceedings of APSEC, 2010 Cloud Workshop, Sydney, Australia.

[11] Kelvin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham, "Security issues for cloud computing", Technical report, University of Texas, Dallas, Feb, 2010.

[12] Ralf L¨ammel, "Google's MapReduce Programming Model—Revisited", Data Programmability Team, Microsoft Corp.,Redmond,WA,USA.

[13] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud Security Issues", IEEE, 2009.

13. ABOUT THE AUTHOR

Er. Soumya Ranjan Jena is presently working as **Teaching Associate** in the department of CSA at **AKS University, Satna**. He has obtained B.Tech in CSE from BPUT, M.Tech in IT from CITE, Utkal University, and CCNA from CTTC. His research interests include Cloud Computing (load balancing, security, and moving data to media cloud), Wireless Networks, Sensor Networks, Mobile Computing, Algorithms, etc.