IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 68-71

A Security Aspects In Cloud Computing

Dr. Girish Katkar[1], Ms. Punam Naphade[2]
[1]*Taywade College, Koradi*
[2]*Research Scholar, RTMNU, Nagpur*

Abstract: *Cloud computing is considered as one of the major shifts in contemporary computing. Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes. The three fundamental classifications are often referred to as the SPI model where SPI refers to Software, Platform And Infrastructure (As a Service) respectively.These three major parts construct the bulk of services in cloud computing environments Although the benefits of these services are obvious, widespread adaptation of cloud computing depends on properly addressing the relevant security challenges. Many of the attacks on cloud computing are related to their distributed and shared environment. Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success End users need to access resources within the cloud and may bear in mind of access agreements like acceptable use or conflict of interest. The client organization have same mechanism to find vulnerable code or protocols at entry points like servers, firewalls, or mobile devices and upload patches on the native system as soon as they are found.*

Keywords: *Cloud Computing, Security, Service, Client, Service Provider*

I. Introduction

Cloud computing is a heterogeneous architecture, benefitting from a range of technologies to provide several remote services. National Institute of Standards and Technology (NIST) has identified five widely accepted characteristics, common to all cloud systems (Vaquero et al., 2008 Mell and Grance, 2009, Hogan et al., 2011). These are on – demand self service, broad network access and diversity of client devices, resource pooling, rapid elasticity and measured service with the pay per use business model. Resource pooling allows the cloud providers to serve multi – tenant clients by managing resource utilization efficiently using virtualization, resource partitioning and workload balancing. Rapid elasticity scales the needed resources in a dynamic manner. Other important features include the heterogeneity on both the provider and the client sides, and multi – provider services. Cloud computing can also be defined as it is a new service, which are the collection of technologies and a means of supporting the use of large scale Internet service for the remote applications with good quality of service (QoS) levels.

Cloud computing is considered as one of the major shifts in contemporary computing. The internet, web applications, cluster computing, terminal services and virtualization have all contributed to cloud computing. They have set the grounds for the remote service clients to utilize distributed computing, resource sharing and pay – as – you go models needed in the cloud architecture (Youseff et al., 2008).

Cloud computing is as many technologies such as Saasi.e, "Software as a Service", Paasi.e, "Platform as a Service", IaaS i.e, Infrastructure as a Service". Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes. Examples of such nodes, include end user computers, data centers, and Cloud Services. We term such a network of nodes as a Cloud. Cloud service delivery is divided among three archetypal models and various derivative combinations. The three fundamental classifications are often referred to as the SPI model where SPI refers to Software, Platform And Infrastructure (As a Service) respectively.

These three major parts construct the bulk of services in cloud computing environments (Vaquero et a., 2008m, Youseffet., al, 2008). One part is referred to as Software – as – a – service (SaaS). This service enables the cloud client machines to use the software on a cloud server, as if it were within their local work environments. Platform – as – a – service (PaaS). Provides software development platforms for clients. This can reduce the overheads associated with maintenance and infrastructure. Infrastructure – as – a – service (IaaS) is the third part. Essentially, IaaS provides software, hardware, and network devices, as virtual but apparently on demand services. For instance, enterprises can get all the benefits associated with a data center, without actually owning and operating one.

Although the benefits of these services are obvious, widespread adaptation of cloud computing depends on properly addressing the relevant security challenges. Many studies and surveys have already established this, for instance see (Hayess, 2008, Takabiet. Al., 2010, Catteddu and Hogben, 2009). Many of the attacks on cloud computing are related to their distributed and shared environment. such attacks may target any networked

system. They may be considered as the more traditional threats that are also of concern in cloud environment (Takabi et. al. 2010). Denial of Service (DoS) attacks or Cross Site Scripting (CSS) threats are examples on this category (Chen et al. 2010). On the other hand, some threats are specific to cloud environments. This may for instance be related to multi – tenancy nature of the cloud server or to virtual machines (VM) that form the basis of the cloud computing paradigm (Chen et al., 2010). In either of these cases, traditional cryptography and its evolutions play dominant roles in addressing some the underlying challenges (Kamara and Lauter, 2010). The issues related to certifying authorities and Public Key Infrastructure (PK) system as well as privacy and authentication management require special attention, More recent approaches like data centric security and Homomorphic cryptography are making substantial progress in addressing cloud security challenges (Gentry and Halevi, 2011). However, to achieve secure remote computing environments, utilization of Homomorphic encryption must be limited to schemes that avoid bootstrapping techniques. That is because, bootstrapping techniques can lead to chosen ciphertext attacks (Chunsheng, 2012, Chun – sheng and ji – xing)

II. Security Issues In Cloud

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success (Khorshed, Ali &Wasimi, 2012). The security challenges for cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security (Teneyuca, 2011). Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated. Cloud users` personal data security is thus a crucial concern in a cloud computing environment (Joint, Baker & Eccles, 2009); Ismail, 2011; King & Raja, 2012). In terms of customers personal or business data security, the strategic policies of the cloud providers are of highest significance (Joint & Baker, 2011) as the technical security solely is not adequate to address the problem. Trust is another problem which raises security concerns to use cloud service (Ryan &Falvy, 2012) for the reason that it is directly related to the credibility and authenticity of the cloud service providers. All kinds of attacks that are applicable to a computer network and the data in transit equally applies to cloud-based services – some threats in this category are man in the middle attack, phishing, eavesdropping, sniffing and other similar attacks. DDoS (Distributed Denial of Service) attack is one common yet major attack for cloud computing infrastructure (Dou, Chen & Chen, 2013). The well-known DDoS attack can be a potential problem for cloud computing, though not with any exception of having no option to mitigate this.

In cloud computing context, a security concern is always some type of risk but any risk cannot be blindly judged to be a security concern. Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities. Like any other network scenario, the provision of insider – attack remains as a valid threat for cloud computing (Ogiagau – Neamtiu, 2012). Any security tools or other kinds of software used in a cloud environment might have security loopholes which in turn would pose security risks to the cloud infrastructure itself. The problem with third party APIs as well as spammers are threats to the cloud environment (Bisong& Rahman, 2011; Singh &Jangwal, 2012).

Different modes of data transfer and communication means (e.g. satellite communication) might need to take into account. Huge amount of data transfer is a common anticipation in a cloud environment, the communication technology used along with the security concerns of the adapted communication technology also becomes a security concern for the cloud computing approach. The broadcast nature of some communication technology is a core concern in this regard (Celesti Fazio, Villari&Puliafito, 2012). Cloud environment is associated with both physical and virtual resources and they pose different level of security issues – having no sophisticated authentication mechanism to fully address the security threats is an existing problem for cloud computing. It has mainly resulted in the situations where grid computing has been taken as an embedded part of cloud computing (Casola, Cuomo, Rak& Villano,2013). As a result, total Internet related security concerns are anticipated to be automatically added on top of the cloud specific security issues. Bringing portability is one of the means of make cloud services flexible. The portability of cloud services would also be associated with security concerns. Cloud portability enables the cloud users to switch among different cloud service providers without being affected with the necessity to change the ways to accomplish tasks in different ways. It is a clear provision on bargaining power for the cloud users; but at the same time, the security issues with cloud portability are to be counted. Cloud portability might bring severe degree of API based security threats (Petcu, Macariu, Panica&Cracium, 2013).

The hierarchical arrangement of cloud computing facilitates different level of extensibility for the cloud users with varying degree of associated security issues (Che et al., 2011). Security issues for cloud computing are described by some authors as an obvious one due to it nature. In a business model, the risks for the

consumers are related to and dependent on the relevant approaches and policies of the cloud service providers the consumers are dealing with. Using cloud products or services may lead to security concerns for the consumers if they are not a well aware with the type and particulars of the products or services they are to procure or to use in a cloud environment; this is also related to the cloud providers' identity and reliability. One of the inherent problems in this context is that , the consumers might normally not be able to identify or foresee all the risks involved in the specific cloud transaction they are dealing with or involved in (Svantesson& Clarke, 2010)

IaaS Security issues

VM security securing the VM operating systems and workloads from common security threats that affect traditional physical servers, such as malware and viruses, using traditional or cloud - oriented security solutions. The VM's security is the responsibility of cloud consumers. Each cloud consumer can use their own security controls based on their needs expected risk level and their security management process.

Securing VM images repository - unlike physical servers VMs are still under risk even when they are offline. VM images can be compromised by injecting malicious codes in the VM file or even stole the VM file itself. Secured VM images repository is the responsibilities of the cloud providers. Another issue related to VM templates is that such templates may retain the original owner information which may be used by a new consumer.

Virtual network security - sharing or network infrastructure among different tenants within the same server (using v switch) or in the physical networks will increase the possibility to exploit vulnerabilities, or even the vswitch software which result in network-based VM attacks.

Securing VM boundaries - VM have virtual boundaries compared with to physical sever ones. VMs that control on the same physical server share the same CPU. Mentory I/O, NIC, and others (i.e. there is no physical isolain among VM resources). Securing VM boundaries is to responsibility of the cloud provider.

Hypervisor security - a hypervisor is the "virtualizer" the maps from physical resources to virtualized resources are vice versa. It is the main controller of any access to the physical server resources by VMs.

PaaS security Issues

SOA related security issues - the PaaS model is based on the service-oriented Architecture (SOA) model. This leads to inherinting all security issues that exist in the SOA domain such as DOS attacks. Mprein the midale XML-related attacks. Replay attacks, Disctonary attacks injection attacks and input validation related attacks PaaS. Mutual authentication authorization and Ws-Secet's standards are important to secure the cloud provider services. This security issue is at shared responsibilities among cloud providers, service providers and consumers API security. PaaS may after APIs that deliver management functions such as business function security, functions application management etc. Such APIs should be provided with security controls and implemented, such as OAuth to enforce consistent authentication and authorization Moreover, there is a need for be isolation of APIs at memory. This issue is under the responsibility of the cloud service provider.

SaaS security issues

In the SaaS model enforcing and maintaining security and shared responsibility among the cloud providers and security providers (software vendors). The SaaS model inherital security issues discussed in the provision two models built on top of both of them including data security management (data locality, integrity, access, confidentiality, backups) and network security.

Web applications scanning - web applications to be hosted on the cloud infrastructure should be validated and scanned for vulnerabilities using web application scanners. Such scanners should be up to date with the recently discovered vulnerabilities and attack paths maintained in the National Vulnerability Database. Web application firewalls should be in place to mitigate existing / discovered vulnerabilities (examining HTTP requests and responses for applications specific vulnerabilities). The ten most critical web applications vulnerabilities in 2010 listed by OWASP are injection, cross site scripting (Input validation) weaknesses.

End user Security Issues

End users need to access resources within the cloud and may bear in mind of access agreements like acceptable use or conflict of interest. The client organization have same mechanism to find vulnerable code or protocols at entry points like servers, firewalls, or mobile devices and upload patches on the native system as soon as they are found.

Security – as –a – service

In cloud environment the security provided by customers using cloud services and the cloud service providers (CSPs). Security – as a service is a security provided as cloud services and it can provide in two

methods: In first method anyone can changing their delivery methods to include cloud services vendors. The second method Cloud Service Providers are providing security only as a cloud service with information security companies.

Browser Security

In a Cloud environment, remote servers are used for computation. The client nodes are used for input/output operations only, and for authorization and authentication of information to the cloud. A Standard Web browser is platform in dependent client software useful for all users throughout the world. This can be categorized into different types: Software as – a – Service (SaaS), Web applications, or Web 2.0 TLS is used for data encryption and host authentication

Authentication

In the cloud environment, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Trusted platform Module (TPM) is a widely available and stronger authentication than username and passwords. Trusted Computing Groups (TCG`s) if IF – MAP standard about authorized users and other security issue in real – time communication between the cloud provider and the customer.

III. Conclusion

Cloud computing is as many technologies such as Saasi.e, "Software as a Service", Paasi.e, "Platform as a Service", IaaS i.e, Infrastructure as a Service".. Many of the attacks on cloud computing are related to their distributed and shared environment. such attacks may target any networked system. They may be considered as the more traditional threats that are also of concern in cloud environment. Denial of Service (DoS) attacks or Cross Site Scripting (CSS) threats are examples on this category. In terms of customers personal or business data security, the strategic policies of the cloud providers are of highest significance as the technical security solely is not adequate to address the problem. In IaaS sharing or network infrastructure among different tenants within the same server (using v switch) or in the physical networks will increase the possibility to exploit vulnerabilities, or even the v switch software which result in network-based VM attacks. Replay attacks, Disctonary attacks injection attacks and input validation related attacks PaaS. In the SaaS model enforcing and maintaining security and shared responsibility among the cloud providers and security providers (software vendors). The SaaS model inherital security issues discussed in the provision two models built on top of both of them including data security management (data locality, integrity, access, confidentiality, backups) and network security.

References

[1]. "Security Architecture of Cloud Computing", V.KRISHNA REDDY 1, Dr. L.S.S.REDDY, International Journal of Engineering Science and Technology (!JEST), Vol. 3 No. 9 September 2011.
[2]. 'The Effective and Efficient Security Services for Cloud Computing ", Sambh ajiSarode, Deepali Giri, Khushbu.
[3]. Chopde, International lournal of Computer Applications (0975 - 8887) Volume 34- No.9, November 2011.
[4]. "Cloud Computing Security" Danish Jamil Hassan Zaki, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4 April 201 I
[5]. Peter Mell, and Tim Grance, "Draft NIST Working Definition of Cloud Computing," 2009
[6]. http://csrc.nist.gov/ groups/SNS/cloud-computing
[7]. "Cloud Computing Security Issues and Challenges", Kuyoro S. 0.,Ibikunle F., Awodele O.
[8]. Catteddu D. 2010 Cloud Computing. [Online] Available from: http://w.enisa.europa.eu/act/rm! files/deliverables
[9]. c1oud-computing risk- assessment [Accessed 26th April 2010]
[10]. http://adventuresinsecurity.comlblognp=67
[11]. http://www.maintec.comlblog/find-your-way-to-securecloud- part-2