A Survey on Security issues in cloud computing

D. Anil Kumar, Y. Manasa

[1]Assistant Professor, Dept of CSE, Qis Institute of Technology, Ongole,

[2]Dept of IT, NRI Institute of Technology, Vijayawada.

anil.dudla@gmail.com, manasa12yadavalli@gmail.com

Abstract: The cloud computing ensures remarkable potential strength to provide elastic, cost effective, easy to manage, and powerful resource management through the internet. The cloud computing, upsurges the capabilities of the hardware resources by optimal and shared utilization. The above feature enables or encourages the individuals and industries to collaborate applications and services with cloud environment. Because of cloud simplicity, it ensures plenty of potential security threats to cloud data storage and applications. This survey provides the details of security issues that arise due to the very nature of cloud computing in very recent years.

1. Introduction

Since its inception, the cloud computing paradigm has gained the widespread popularity in the industry and academia [1]. The economical, scalable, expedient, ubiquitous, and on-demand access to shared resources are some of the characteristics of the cloud that have resulted in shifting the business processes to the cloud [2]. The cloud computing attracts the attention of research community due to its potential to provide tremendous benefits to the industry and the community [9]. The resources are provided to the users and released based on demands from the pool of shared resources [4]. The on-demand resource provisioning ensures the optimal resource allocation and is also cost effective. The consumers (individuals and business organizations) no longer need to invest heavily in the information technology (IT) infrastructure [4]. Customers use resources provided by the cloud and pay according to the use. On the other hand, cloud providers can re-use resources as soon as they are released by a particular user resulting in improved resource utilization. Ease of use is yet another advantage being offered by the cloud computing because it does not require the customers to possess extraordinary expertise pertaining to the cloud specific technologies [5]. The management of the technology and services has moved from user to the service provider's end [5].There are various studies in the literature discussing the security issues of the cloud computing. The authors in [5,10] presented reviews on the security issues of the cloud computing. However, the aforesaid studies are limited to the discussion of security issues only and the security solutions are not discussed. Ref. [11] reviewed the security issues at different levels of cloud computing. The security solutions have also been presented in [11]. However, the future discussion has not been discussed comprehensively and overview of the cloud technology is missing. The authors in [1] presented a comprehensive study of privacy preservation in the cloud with focus only on e-health clouds. Moreover, the study in [1] is limited in scope to the privacy only.

2. CLOUD COMPUTING ARCHITECTURAL FRAMEWORK

Cloud computing integrates various computing technologies to provide services to the end users. To understand the security issues pertaining to the cloud computing, it is important to briefly introduce the concepts that contribute to the cloud computing. The National Institute of Standards and Technology's (NIST) definition [69] of cloud computing is widely accepted [2]. The NIST definition considers the cloud computing as a threefold model of service provisioning (Fig. 1), comprising of: (a) essential characteristics, (b) service models, and (c) deployment models. The cloud computing concepts in the light of NIST definition are presented below.

2.1. CHARACTERISTICS

2.1.1. On-demand self-service

Customers can request and manage the services from the cloud without any human interaction with the CSP. The provision of the services and the associated resources is accomplished as and when required. This is usually done through Web services and management interfaces [2].

2.1.2. Broad network access

The services and the customer's applications and data present on the cloud must be accessible to the customers using the standard mechanisms and protocols. The characteristic further demands that the availability of services should support heterogeneous thin or thick environment (for example, mobile phones, laptops, workstations, tablets). Broad network access is sometimes referred to as ubiquitous network access in the literature [2].

2.1.3. Resource pooling

The cloud's resources are shared among multiple customers by pooling in a multi-tenant environment. The customers are transparent about the location of the resources. There is a mapping between physical and virtual resources provided to the customers.

2.1.4. Rapid elasticity

The resources can be rapidly and elastically scaled as per customer's demands. The customer has a view of unlimited resources that can be purchased as needed in a pay-as-you-go manner.

2.1.5. Measured service

The scaling of resources up and down is performed dynamically and the usage of services is metered and reported to the customer and CSP. The metering also helps the optimization of resource usage automatically while the users are charged in a pay-as-you-use manner.

2.1.6. Multi-tenancy

The NIST defines the above mentioned five characteristics of the cloud computing. However, the Cloud Security Alliance (CSA) adds multi-tenancy as an important characteristic of the cloud computing (although not an essential characteristic)

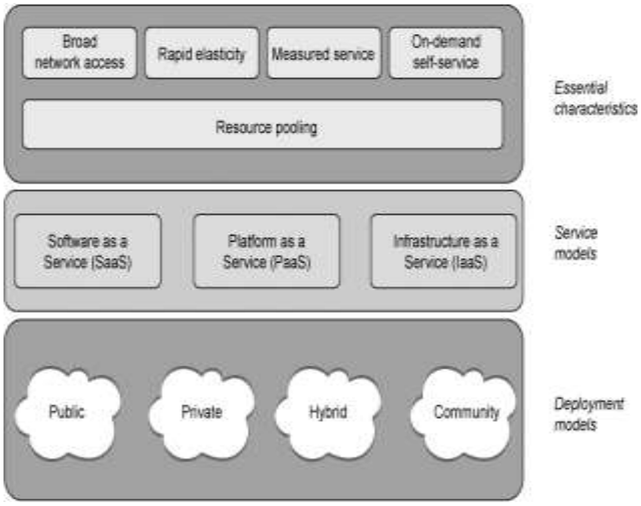

Fig. 1 NIST definition of cloud computing.

Multi-tenancy is the property that enables the use of a single resource by multiple customers that may or may not belong to the same organization. Multi-tenancy results in optimal use of resources and different customers are segregated logically.

2.2. SERVICE MODELS

The NIST divides the services provided by the cloud computing into three categories, namely: (a) software as a service (SaaS), (b) platform as a service (PaaS), and (c) infrastructure as a service (IaaS). The cloud service model is referred to as SPI (software, platform, and infrastructure).

2.2.1. SaaS

The SaaS enables the customers to use CSP’s applications, running on the cloud infrastructure, through the Internet. The thin client interface can be used to access the applications such as web browser. The SaaS does not provide the facility to create an application or software. The SaaS only provides software through Internet making it a model to distribute the software through Web. The customers pay for the usage and do not own the software [6].

2.2.2. PaaS

The applications that are owned by the customer need a frame work where they can be executed and managed. This includes integrated development environments (IDE), operating systems, and platform layer resources (run time engine that executes the applications). The aforementioned services are provided as PaaS. The PaaS does not provide customers with the control over the underlying cloud infrastructure but only on the applications that are moved to the cloud.

2.2.3. IaaS

The IaaS refers to the hardware infrastructure provided by the CSP including the network, storage, memory, processor, and various other computing resources. The resources are provided in the form of virtualized systems accessible through Internet. The CSP has a control over the underlying resources [9].

2.3. DEPLOYMENT MODELS

There are four models that can be used to deploy a cloud computing infrastructure, namely: (a) private cloud, (b) public cloud, (c) community cloud, and (d) hybrid cloud.

2.3.1. Private cloud

The cloud that is run and managed only for a single organization is the private cloud. The organization may or may not own the physical infrastructure and can be managed by the organization itself or by a third party. Similarly, private cloud may or may not be located at organization's geographical site. However, whatever the case may be, private cloud is for the use of only single organization and the resources are not utilized by any other customer.

2.3.2. Public cloud

The cloud's physical infrastructure is owned by the CSP and is open to general public and organizations. The resources are shared among all the customers. The customers pay the cloud owner according to the services and resources they use. The physical infrastructure is located off-site to the customers and is managed by the CSP.

2.3.3. Community cloud

The community cloud is shared by a number of organizations and/or customers forming a community. Generally, the community shares common interests, such as the mission, security requirements, policy, and compliance considerations. The community cloud may be managed by any of the organizations in the community or a third party. Similarly, it may be located on premise or off-premise**.**

2.3.4. Hybrid cloud

The hybrid cloud is the mix of two or more clouds (public, private, or community). All of the participating clouds retain their status of a unique entity, but share standardized or proprietary technology.

3. CLOUD SECURITY CHALLENGES

3.1 VIRTUALIZATION ISSUES

Virtualization is one of the strategic components of the cloud. Virtualization allows the use of same physical resources by multiple customers. A separate VM is instantiated for each user that virtually provides a complete operating machine to the user [7]. Several VMs can be mapped to the same physical resources allowing the resource pooling in multi-tenant environment. A VM monitor (VMM) or hypervisor is the module that manages the VMs and permits various operating systems to run simultaneously on the same physical system [7]. Nevertheless, virtualization also introduces security challenges to the cloud users and infrastructure [8]. We discuss the security issues related to virtualization below.

3.1.1 VM image sharing.

A VM image is used to instantiate VMs. A user can create his/her own VM image or can use an image from the shared image repository [9]. The users are allowed to upload and download images from the repository (for example Amazons image repository) [9]. Sharing of VM images in the image repositories is a common practice and can evolve as a serious threat if it is used in malicious manner [4]. A malicious user can investigate the code of the image to look for probable attack point. On the other hand, a malicious user can upload an image that contains a malware [7]. The VM instantiated through the infected VM image will become source of introducing malware in the cloud computing system. Moreover, an infected VM can be used to monitor the activities and data of other users resulting in privacy breach. Likewise, if the image is not properly cleaned, it can expose some confidential information of the user [3].

3.1.2. VM isolation.

VMs running on the same physical hardware need to be isolated from each other. Although logical isolation is present between different VMS, the access to same physical resources can lead to data breach and cross-VM attacks. Isolation is not only needed on storage devices but memory and computational hardware also needs fine grained isolation of VMs [1].

3.1.3. VM escape.

VM escape is a situation in which a malicious user or VM escapes from the control of VMM or hypervisor [7]. A VMM is a software component that manages all the VMs and their access to the hardware. The VM escape situation can provide attacker access to other VMs or can bring the VMM down [4]. A successful VM escape attack can provide access to the computing and storage hardware. The IaaS service model is affected that can in turn effect other service models [3].

3.1.4. VM migration.

The VM migration is the process of relocating a VM to another physical machine without shutting down the VM [8]. The VM migration is carried out for a number of reasons, such as load balancing, fault tolerance, and maintenance [3]. During the migration phase, the contents of the VM are exposed to the network that might lead to data privacy and integrity concerns. Besides data, the code of VM also becomes vulnerable to attackers during migration [4]. The migration module can be compromised by an attacker to relocate the VM to a compromised server or under the control of compromised VMM. The VM migration is a crucial phase and needs to be carried out in a secured manner [9].

3.1.5. VM rollback.

Virtualization allows the rollback of a VM to some previous state whenever it is needed. The rollback feature provides flexibility to the user. However, rollback also raises security concerns [9]. For example, the rollback can enable the security credentials that were previously disabled [9]. Moreover, the rollback can also render the VM to a vulnerability that was previously patched [16]. Furthermore, the rollback can revert the VM to previous security policies and configuration errors [9].

3.1.6. Hypervisor issues.

The key module of virtualization is hypervisor or VMM. The VMs management and isolation is the responsibility of the VMM. Generating and managing virtual resources, is yet another function performed by the VMM. A VMM may affect the execution of VMs running on the host system [10]. A compromised VMM can put all the VMs that are managed by the victim VMM under attacker’s control [1]. The metadata of the VMs, kept by the VMM, may also be exposed to an attacker if the attacker takes control of a VMM [1,10]. A VMM can provide larger attack vector due to more entry points and interconnection complexities [10]. There are many reported bugs in the VMM that let the attacker to take control of the VMM or bypass security restrictions. For example, vulnerabilities in the Xen, Microsoft Virtual PC, and Microsoft Virtual Server can be abused by attackers to gain privileged rights [12].

3.1.7. VM sprawl.

VM sprawl is a situation where a number of VMs on the host system is continuously increasing and most of the already instantiated VMs are in idle state [8]. The VM sprawl causes the resources of the host machine to be wasted on large scale [9].

3.2. DATA/STORAGE ISSUES

The cloud computing model does not deliver users with full control over data. Distinct to conventional computing model, the cloud computing permits the service providers to exercise control to manage servers and data. The user enjoys certain level of control only on the VMs [14]. The lack of control over the data results in greater data security risks than the conventional computing model. Moreover, the characteristics of cloud computing like multi-tenancy and virtualization also come up with the possibilities of attacks different than the conventional computing model. Below we provide an overview of the security challenges faced by the data in cloud computing environment.

3.2.1. Data privacy and integrity.

Although the cloud computing ensures the cost economy and also relieves the users from infrastructure management activities, it also entails security issues. The data in the cloud is much more vulnerable to risks in terms of confidentiality, integrity, and availability in comparison to the conventional computing model [11]. The ever increasing number of users and applications leads to enhanced security risks. In a shared environment, the security strength of the cloud equals the security strength of its weakest entity [3]. Not only the malicious entity collocated with the victim data, but also any non-malicious but unsecure entity can result in breach of data. A successful attack on a single entity will result in unauthorized access to the data of all the users. Violation of integrity may also result from multi-tenant nature of the cloud. Employee of SaaS providers, having access to information may also act as a potential risk [39]. Besides the data at rest, the data being processed also comes across security risks [9]. Due to virtualization physical resources are shared among multiple tenants. This eventually may allow malicious users (sharing computing resources) to launch attacks on the data of other users while in processing phase [5]. Moreover, if the data backup process is outsourced to a third party by the CSP, risks boundary is also broadened. The cryptographic key generation and management for cloud computing paradigm is also not standardized. Absence of secure and standard key management techniques for the cloud does not allow the standard cryptographic mechanisms to scale well to the cloud computing model [7]. Therefore, domain of cryptography also enhances the potential risks to the data.

3.2.2. Data recovery vulnerability.

Due to resource pooling and elasticity characteristics, the cloud ensures dynamic and on demand resource provisioning to the users. The resource allocated to a particular user may be assigned to the other user at some later point of time. In case of memory and storage resources, a malicious user can employ data recovery techniques to obtain the data of previous users [10]. The authors in [10] were able to recover Amazon machine images files 98 % of the times. The data recovery vulnerability can pose major threats to the sensitive user data [7].

3.2.3. Improper media sanitization.

The issue is related to the destruction of physical storage media due to a number of reasons, for example, (a) the disk needs to be changed, (b) the data no longer needs to be there, and (c) termination of service [7]. If the CSP does not sanitize the devices properly, the data can be exposed to risks [7]. Sometimes, the multi-tenancy also contributes to the risk of device sanitization. At the end of the device life cycle, it may not be possible to destroy it as it is in use of some tenants [8].

3.2.4. Data backup.

The data backup is also an important issue that needs to be dealt carefully. A regular data backup is needed at the CSP side to ensure the availability and recovery of data in case of intentional and accidental disasters. Moreover, the backup storage also needs to be protected against unauthorized access and tampering [11].

3.3. WEB APPLICATION AND APPLICATION PROGRAMMING INTERFACE (API) SECURITY

As discussed in Section 1, services and applications to the cloud users are provided through the Internet [16]. In fact, it is one of the essential requirements for a cloud application to be utilized and managed over the Web [11]. The application provided by the CSP is always located at the cloud with users accessing it ubiquitously. One of the important characteristics of cloud applications is that they are not bonded with specific users [10]. Different users may access the same application possibly at the same time. The cloud applications inherit the same vulnerabilities as traditional Web applications and technology. However, the traditional security solutions are not adequate for the cloud computing environment because the vulnerabilities in web application in cloud can prove to be far more devastating than the traditional Web applications. Co-location of multiple users, their data, and other resources makes it much greater issue. The top ten risks in the web applications have been identified by Open Web Application Security Project in 2013 to be the following [7]. Injection (SQL, OS, and LDAP) Broken Authentication and Session Management Cross-Site Scripting (XSS) Insecure Direct Object References Security Misconfiguration Sensitive Data Exposure Missing Function Level Access Control Cross-Site Request Forgery (CSRF) Using Known Vulnerable Components Invalidated Redirects and Forwards The development, management, and use of Web applications must take into consideration the above given risks to safeguard the web applications and users resources. The user and the services in the cloud are bridged by the APIs. The security of APIs highly influences the security and availability of the cloud services [10]. The secure APIs ensure the protected and non-malicious use of the cloud services [11]. An API can be thought of a user guide that describes the details about the CSPs cloud architecture and features. The users build or extend the services using the APIs [11]. The CSPs usually publish their APIs to market the features of their cloud. At one hand, the publishing of APIs helps the users to know the details about the components and functions of the cloud. On the other hand, the cloud architecture to some extent is exposed to the attackers

[10]. Therefore, insecure APIs can be troublesome for both the cloud and the users. The vulnerabilities of APIs include weak credentials, insufficient authorization and input-data validation. Moreover, the frequent updates of APIs may introduce security holes in the applications [14].

3.4. IDENTITY MANAGEMENT AND ACCESS CONTROL

In a cloud environment, the confidentiality and integrity of data and services is also linked with the identity management and access control. It is exceptionally important to keep track of the user's identity and controlling unauthorized access to the information [16]. The issue of identity management and access control becomes more complex in a cloud environment due to the fact that the owner and resources are in different administrative domains and organization's authentication and authorization may not be exported to the cloud in the existing.

4. CONCLUSION

This survey presented the security issues that arise due to the shared, virtualized, and public nature of the cloud computing paradigm. Subsequently, the counter measures presented in the literature are presented. The tabulated analysis of the presented techniques highlighted the scope of security services provided by the reviewed techniques. Tabulated analysis will greatly help the readers to compare and analyze the pros and cons of the research endeavors. Due to increased use of smart phones and mobile devices, the MCC has also taken off. We briefly discuss the security concerns of the MCC. The discussion of the presented technique has led ways to highlight some open issues to motivate the research community and academia to focus on the subject.

5. REFERENCES

[1] A. Abbas, S.U. Khan, A review on the state-of-the-art privacy preserving approaches in e-health clouds, IEEE J. Biomed. Health Inform. (2014).

[2] M. Aslam, C. Gehrmann, M. Bjorkman, Security and trust preserving VM migrations in public clouds, in: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 869–876.

[3] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, M. Xu, Web services agreement specification (WSagreement),

[4] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing, 2012, pp. 1427–1434.

[5] S. Carlin, K. Curran, Cloud computing security, Int. J. Ambient Comput. Intell. 3 (1) (2011) 14–19.

[6] R. Chandramouli, M. Iorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing, Springer, New York, 2014, pp. 1–30. doi: 10.1007/978-1-4614-9278-8_1.

[7] S. Chaisiri, B. Lee, D. Niyato, Optimization of resource provisioning cost in cloud computing, IEEE Trans. Services Comput. 5 (2) (2012) 164–177.

[8] D. Chen, H. Zhao, Data security and privacy protection issues in cloud computing, in: International Conference on Computer Science and Electronics Engineering (ICCSEE, IEEE), vol. 1, 2012, pp. 647–651.

[9] R. Bobba, H. Khurana, M. Prabhakaran, Attribute-sets: a practically motivated enhancement to attribute-based encryption, in: Computer Security ESORICS, Springer, Berlin, Heidelberg, 2009, pp. 587–604.

[10] J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Proc. Eng. 23 (2011) 586–593.

[11] A. Corradi, M. Fanelli, L. Foschini, VM consolidation: a real case based on openstack cloud, Future Gener. Comput. Syst. 32 (2014) 118–127.

[12] Y. Fu, Z. Lin, Exterior: using a dual-vm based external shell for guest-os introspection, configuration, and recovery, in: Proceedings of the 9th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, 2013, pp. 97–110.

[13] J. Groth, Amit Sahai, Efficient non-interactive proof systems for bilinear groups, in: Advances in Cryptology EUROCRYPT, Springer, Berlin, Heidelberg, 2008, pp. 415–432.

[14] N. Gonzalez, C. Miers, F. Redgolo, M. Simplcio, T. Carvalho, M. Nslund, M. Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing, J. Cloud Comput. 1 (1) (2012) 1–18.

[15] M. Ficco, M. Rak, Stealthy denial of service strategy in cloud computing, IEEE Trans. Cloud Comput. (2014).

[16] C. Wang et al., “Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,” Proc. IEEE INFOCOM ‘10, Mar. 2010.