IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

Cloud Computing Security Problem Analysis

Ashish Singh[1], Anant Singh[2], Pulkit Mittal[3], Mr. Gaurav Chaudhary[4]
Students, Department of Computer Science and Information Technology[1,2,3]
Assistant Professor, Department of Computer Scienceand Information Technology[4]
Dronacharya Group of Institutions, Greater Noida, U.P., India

I. INTRODUCTION

A common understanding of "cloud computing" is continuously evolving, and the terminology and concepts used to define it often need clarifying. Press coverage can be vague or may not fully capture the extent of what cloud computing entails or represents, sometimes reporting how companies are making their solutions available in the "cloud" or how "cloud computing" is the way forward, but not examining the characteristics, models, and services involved in understanding what cloud computing is and what it can become. This white paper introduces internet- based cloud computing, exploring the characteristics, service models, and deployment models in use today, as well as the benefits and challenges associated with cloud computing. Also discussed are the communications services in the cloud (including ways to access the cloud, such as web APIs and media control interfaces) and the importance of scalability and flexibility in a cloud-based environment. Also noted for businesses desiring to start using communication services, are the interface choices available, including Web 2.0 APIs, media control interfaces, Java interfaces, and XML based interfaces, catering to a wide range of application and service creation developers.

The term "cloud", as used in this white paper, appears to have its origins in network diagrams that represented the internet, or various parts of it, as schematic clouds. "Cloud computing" was coined for what happens when applications and services are moved into the internet "cloud." Cloud computing is not something that suddenly appeared overnight; in some form, it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications. Many companies are delivering services from the cloud. Some notable examples include the following

- **Google** — Has a private cloud that it uses for delivering Google Docs and many other services to its users, including email access, document applications, text translations, maps, web analytics, and much more.
- **Microsoft** — Has Microsoft® Office 365® online service that allows for content and business intelligence tools to be moved into the cloud, and Microsoft currently makes its office applications available in a cloud.
- **Salesforce.com** — Runs its application set for its customers in a cloud, and its Force.com and Vmforce.com products provide developers with platforms to build customized cloud services. But, what is cloud computing? The following sections note cloud and cloud computing characteristics, services models, deployment models, benefits, and challenges. Characteristics Cloud computing has a variety of characteristics, with the main ones being:
- **Shared Infrastructure** — Uses a virtualized software model, enabling the sharing of physical services, storage, and networking capabilities. The cloud infrastructure, regardless of deployment model, seeks to make the most of the available infrastructure across a number of users.
- **Dynamic Provisioning** — Allows for the provision of services based on current demand requirements. This is done automatically using software automation, enabling the expansion and contraction of service capability, as needed. This dynamic scaling needs to be done while maintaining high levels of reliability and security.
- **Network Access** — Needs to be accessed across the internet from a broad range of devices such as PCs, laptops, and mobile devices, using standards-based APIs (for example, ones based on HTTP). Deployments of services in the cloud include everything from using business applications to the latest application on the newest smartphones.
- **Managed Metering** — Uses metering for managing and optimizing the service and to provide reporting and billing information. In this way, consumers are billed for services according to how much they have actually used during the billing period.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

II. Literature Review

Cloud computing security challenges and issues discussed by various researchers. The Cloud Computing Use Cases group [4] discusses the different use case scenarios and related requirements that may exist in the cloud computing model. They consider use cases from different perspectives including customers, developers and security engineers. ENISA [5] investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in cloud computing that may lead to such risks. Similar efforts discussed in "Top Threats to Cloud Computing" by CSA [6]. Balachandra et al [7] discuss the security SLA's specifications and objectives related to data locations, segregation and data recovery. Kresimir et al [8] discuss high level security concerns in the cloud computing model such as data integrity, payment, and privacy of sensitive information. Kresimir discussed different security management standard s such as ITIL, ISO/IEC 27001 and Open Virtualization Format (OVF). Meiko et al [9] discuss the technical security issues arising from adopting the cloud computing model such as XML-attacks, Browsers' related attacks, and flooding attacks. Bernd et al [10] discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology-related, cloud characteristics -related, security controls- related. Subashini et al [11] discuss the security challenges of the cloud service delivery model, focusing on the SaaS model. CSA [6] discusses critical areas of cloud computing. They deliver a set of best practices for the cloud provider, consumers and security vendors to follow in each domain. CSA published a set of detailed reports discussing for some of these domains.

In our research we did a deep investigation in the cloud model to identify the root causes and key participating dimensions in such security issues/problems discussed by the previous work. This will help better to understand the problem and deliver solutions.

III. The Cloud Computing Architecture and Security Implications

The Cloud Computing model has three service delivery models and main three deployment models [1]. The deployment models are: (1) Private cloud: a cloud platform is dedicated for specific organization, (2) Public cloud: a cloud platform available to public users to register and use the available infrastructure, and (3) Hybrid cloud: a private cloud that can extend to use resources in public clouds. Public clouds are the most vulnerable deployment model because they are available for public users to host their services who may be malicious users. The cloud service delivery models, as in figure1, include:

- **Infrastructure-as-a-service (IaaS):** where cloud providers deliver computation resources, storage and network as an internet-based services. This service model is based on the virtualization technology. Amazon EC2 is the most familiar IaaS provider.
- **Platform-as-a-service (PaaS):** where cloud providers deliver platforms, tools and other business services that enable customers to develop, deploy, and manage their own applications, without installing any of these platforms or support tools on their local machines. The PaaS model may be hosted on top of IaaS model or on top of the cloud infrastructures directly. Google Apps and Microsoft Windows Azure are the most known PaaS.
- **Software-as-a-service (SaaS):** where cloud providers deliver applications hosted on the cloud infrastructure as internet-based service for end users, without requiring installing the applications on the customers' computers. This model may be hosted on top of PaaS, IaaS or directly hosted on cloud infrastructure. SalesForce CRM is an example of the SaaS provider.

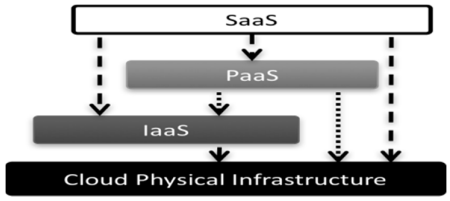

Figure 1: Cloud service delivery models

Each service delivery model has different possible implementations, as in figure 1, which complicates the development of standard security model for each service delivery model. Moreover, these service delivery models may coexist in one cloud platform leading to further complication of the security management process.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

IV. Cloud Computing Characteristics And Security Implications

To achieve efficient utilization of resources, cloud providers need to increase their resource utilization while decreasing cost. At the same time consumers need to use resources as far as needed while being able to increase or decrease resources consumption based on actual demands. The cloud computing model meets such needs via a win- win solution by delivering two key characteristics: multi- tenancy and elasticity. Both characteristics turn out to have serious implications on the cloud model security.

Multi-tenancy implies sharing of computational resources, storage, services, and applications with other tenants. Multi-tenancy has different realization approaches as shown in figure 2. In approach 1, each tenant has their own dedicated instance with their own customizations (customization may include special development to meet customer needs). In approach 2, each tenant uses a dedicated instance, like approach 1, while all instances are the same but with different configurations (adjustment of application parameters or interfaces). In approach 3, all tenants share the same instance with runtime configuration (the application is divided into core application component and extra components that are loaded based on the current tenant requests – similar to SalesForce.com). In approach 4 tenants are directed to a load balancer that redirects tenants requests to a suitable instance based on current instances load. Approaches 3 and 4 are the most risky as tenants are coexisting on the same process in memory and hardware. This sharing of resources violates the confidentiality of tenants' IT assets which leads to the need for secure multi- tenancy. To deliver secure multi-tenancy there should be isolation among tenants' data (at rest, processing and transition) and location transparency where tenants have no knowledge or control over the specific location of their resources (may have high level control on data location such as country or region level), to avoid planned attacks that attempt to co-locate with the victim assets [12]. In IaaS, isolation should consider VMs' storage, processing, memory, cache memories, and networks. In PaaS, isolation should cover isolatation among running services and APIs' calls. In SaaS, isolation should isolate among transactions carried out on the same instance by different tenants and tenants' data.

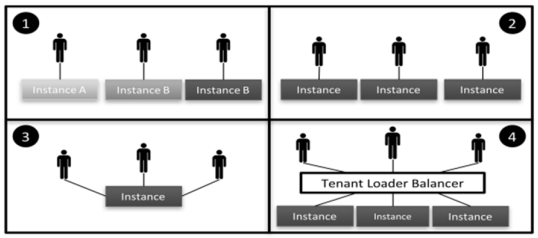

Figure 2: Multi-tenancy approaches [13]

Elasticity implies being able to scale up or down resources assigned to services based on the current demand. Scaling up and down of tenant's resources gives the opportunity to other tenants to use the tenant previously assigned resources. This may lead to confidentiality issues. For example, tenant A scaled down so it releases resources, these resources are now assigned to tenant B who in turn use it to deduce the previous contents of tenant A (similar to lag problem between DNS and DNS cache). Moreover, Elasticity includes a service placement engine that maintains a list of the available resources from the provider's offered resources pool. This list is used to allocate resources to services. Such placement engines should incorporate cloud consumers' security and legal requirements such as avoid placing competitors services on the same server, data location should be within the tenants' country boundaries. Placement engines may include a migration strategy where services are migrated from physical host to another or from cloud to another in order to meet demands and efficient utilization of the resources. This migration strategy should take into account the same security constraints. Furthermore, security requirements defined by service consumers should be migrated with the service and initiates a process to enforce security requirements on the new environment, as defined by cloud consumers, and updates the current cloud security model.

V. Cloud Computing's Deep Dependencies Stack

The cloud computing model depends on a deep stack of dependent layers of objects (VMs, APIs, Services and Applications) where the functionality and security of a higher layer depends on the lower ones. The IaaS model covers cloud physical infrastructure layer (storage, networks and servers), virtualization layer (hypervisors), and virtualized resources layer (VMs, virtual storage, virtual networks). The PaaS model covers the platform layers (such as application servers, web servers, IDEs, and other tools), and APIs and Services layers. The PaaS layer depends on the virtualization of resources as

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

delivered by IaaS. The SaaS model covers applications and services offered as a service for end users, as shown in figure 3. The SaaS layer depends on a layer of platforms to host the services and a layer of virtualization to optimize resources utilization when delivering services to multi-tenant.

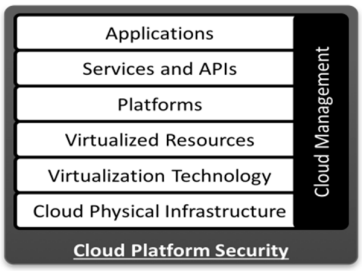

Figure 3: Cloud computing model layers

This deep dependency stack of cloud objects complicates the cloud security problem as the security of each object/layer depends on the security of the lower objects/layers. Furthermore, any breach to any cloud objects will impact the security of the whole cloud platform. Each cloud layer/object has a set of security requirements and vulnerabilities so it requires a set of security controls to deliver secured service. This results in a huge number of security controls that needs to be managed. Moreover, managing such heterogeneous security controls to meet security needs is a complex task, taking into account conflicts among the security requirements and among security controls at each layer. This may result in an inconsistent security model. Hence, a unified security control management module is required. This module should coordinate and integrate among the various layers' security controls based on security needs.

VI. Cloud Computing Stakeholders And Security Implications

The cloud computing model has different involved stakeholders: cloud provider (an entity that delivers infrastructures to the cloud consumers), service provider (an entity that uses the cloud infrastructure to deliver applications/services to end users), and service consumer (an entity that uses services hosted on the cloud frastructure). Each stakeholder has their own security management systems/processes and each one has their own expectations (requirements) and capabilities (delivered) from/to other stakeholders. This leads to:

(1) A set of security requirements defined on a service by different tenants that may conflict with each other. So security configurations of each service should be maintained and enforced on the service instances level and at runtime taking into account the possibility of changing requirements based on current consumers' needs to mitigate new risks;

(2) Providers and consumers need to negotiate and agree on the applied security properties. However, no standard security specification notations are available that can be used by the cloud stakeholders to represent and reason about their offered/required security properties; and

(3) Each stakeholder has their own security management processes used to define their assets, expected risks and their impacts, and how to mitigate such risks. Adopting cloud model results in losing control from both involved parties, including cloud providers (who are not aware of the contents and security requirements of services hosted on their infrastructures) and cloud consumers (who are not able to control neither on their assets security nor on other services sharing the same resources). Security SLA management frameworks represent part of the solution related to security properties specification, enforcement and monitoring. However, SLAs still don't cover security attributes in their specifications [14]. Moreover, SLAs are high level contracts where the details of the security policies and security control and how to change at runtime are not included.

On the other side, cloud providers are not able to deliver efficient and effective security controls because they are not aware of the hosted services' architectures. Furthermore, cloud providers are faced with a lot of changes to security requirements while having a variety of security controls deployed that need to be updated. This further complicates the cloud providers' security administrators' tasks. Transparency of what security is enforced, what risks exist, and what breaches occur on the cloud platform and the hosted services must exist among cloud providers and consumers. This is what is called "trust but verify" [15], where cloud consumers should trust in their providers meanwhile cloud providers should deliver tools to help consumers to verify and monitor security enforcements.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

VII. Cloud Computing Service Delivery Models And Security Implications

We summarize the key security issues/vulnerabilities in each service delivery model. Some of these issues are the responsibility of cloud providers while others are the responsibility of cloud consumers.

7.1 IaaS 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 own 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 of network infrastructure among different tenants within the same server (using vSwitch) or in the physical networks will increase the possibility to exp loit vulnerabilities in DNS servers, DHCP, IP protocol vulnerabilities, or even the vSwitch software which result in network -based VM attacks.
- **Securing VM boundaries** - VMs have virtual boundaries compared with to physical server ones. VMs that co-exist on the same physical server share the same CPU, Memory, I/O, NIC, and others (i.e. there is no physical isolation among VM resources). Securing VM boundaries is the responsibility of the cloud provider.
- **Hypervisor security** - a hypervisor is the "virtualizer" that maps from physical resources to virtualized resources and vice versa. It is the main controller of any access to the physical server resources by VMs. Any compromise of the hypervisor violates the security of the VMs because all VMs operations become traced unencrypted. Hypervisor security is the responsibility of cloud providers and the service provider. In this case, the SP is the company that delivers the hypervisor software such as VMware or Xen.

7.2 PaaS Security Issues

- **SOA related security issues** – the PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting 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 [9, 16]. Mutual authentication, authorization and WS-Security standards are important to secure the cloud provided services. This security issue is a shared responsibility among cloud providers, service providers and consumers.
- **API Security** - PaaS may offer APIs that deliver management functions such as business functions, security functions, application management, etc. Such APIs should be provided with security controls and standards implemented, such as OAuth [17], to enforce consistent authentication and authorization on calls to such APIs. Moreover, there is a need for the isolation of APIs in memory. This issue is under the responsibility of the cloud service provider.

7.3 SaaS Security Issues

In the SaaS model enforcing and maintaining security is a shared responsibility among the cloud providers and service providers (software vendors). The SaaS model inherits the security issues discussed in the previous two models as it is built on top of both of them including data security management [11] (data locality, integrity, segregation, access, confidentiality, backups) and network security. Web application vulnerability scanning - web applications to be hosted on the cloud infrastructure should be validated and scanned for vulnerabilities using web application scanners [18]. Such scanners should be up to date with the recently discovered vulnerabilities and attack paths maintained in the National Vulnerability Database (NVD) and the Common Weaknesses Enumeration (CWE) [19]. 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 [20] are injection, cross site scripting (Input validation) weaknesses.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

Web application security miss-configuration and breaking - web application security miss-configuration or weaknesses in application-specific security controls is an important issue in SaaS. Security miss-configuration is also very critical with multi-tenancy where each tenant has their own security configurations that may conflict with each other leading to security holes. It is mostly recommended to depend on cloud provider security controls to enforce and manage security in a consistent, dynamic and robust way.

7.4 Cloud Management Security Issues

The Cloud Management Layer (CML) is the "microkernel" that can be extended to incorporate and coordinate different components. The CML components include SLA management, service monitoring, billing, elasticity, IaaS, PaaS, SaaS services registry, and security management of the cloud. Such a layer is very critical since any vulnerability or any breach of this layer will result in an adversary having control, like an administrator, over the whole cloud platform. This layer offers a set of APIs and services to be used by client applications to integrate with the cloud platform. This means that the same security issues of the PaaS model apply to the CML layer as well.

7.5 Cloud Access Methods Security Issues

Cloud computing is based on exposing resources over the internet. These resources can be accessed through (1) web browsers (HTTP/HTTPS), in case of web applications - SaaS; (2) SOAP, REST and RPC Protocols, in case of web services and APIs – PaaS and CML APIs; (3) remote connections, VPN and FTP in case of VMs and storage services – IaaS. Security controls should target vulnerabilities related to these protocols to protect data transferred between the cloud platform and the consumers.

VIII. Conclusion

The cloud computing model is one of the promising computing models for service providers, cloud providers and cloud consumers. But to best utilize the model we need to block the existing security holes. Based on the details explained above, we can summarize the cloud security problem as follows:

Some of the security problems are inherited from the used technologies such as virtualization and SOA. Multi-tenancy and isolation is a major dimension in the cloud security problem that requires a vertical solution from the SaaS layer down to physical infrastructure (to develop physical alike boundaries among tenants instead of virtual boundaries currently applied).

Security management is very critical to control and manage this number of requirements and controls. The cloud model should have a holistic security wrapper, as shown in figure 3, such that any access to any object of the cloud platform should pass through security components first.

Based on this discussion we recommend that cloud computing security solutions should:

Focus on the problem abstraction, using model-based approaches to capture different security views and link such views in a holistic cloud security model.

Inherent in the cloud architecture. Where delivered mechanisms (such as elasticity engines) and APIs should provide flexible security interfaces.

Support for: multi-tenancy where each user can see only his security configurations, elasticity, to scale up and down based on the current context.

Support integration and coordination with other security controls at different layers to deliver integrated security. Be adaptive to meet continuous environment changes and stakeholders needs.

Acknowledgements

We thank Dronacharya Group of Institutions for support for parts of this research.

References

[1]. Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def- v15.pdf, Accessed April 2010.

[2]. Frank Gens, Robert P Mahowald and Richard L Villars. (2009, IDC Cloud Computing 2010.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

[3]. IDC, "IDC Ranking of issues of Cloud Computing model," ed, 2009, http://blogs.idc.com/ie/?p=210, Accessed on July 2010.

[4]. Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases Version 3.0," 2010.

[5]. ENISA, "Cloud computing: benefits, risks and recommendations for information security," 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud- computing-risk-assessment, Accessed On July 2010.

[6]. Cloud Security Alliance (CSA). (2010). Available: http://www.cloudsecurityalliance.org/

[7]. Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu Rakshit, "Cloud Security Issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, 2009, pp. 517-520.

[8]. Kresimir Popovic , Zeljko Hocenski, "Cloud computing security issues and challenges," in The Third International Conference on Advances in Human- oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

[9]. Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore 2009, pp. 109- 116.

[10]. Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, "Understanding Cloud- Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.

[11]. S. Subashini, ,Kavitha, V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. In Press, Corrected Proof.

[12]. Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," presented at the Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2009.

[13]. Microsoft. (2006, October, 2010). Multi-Tenant Data Architecture. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx

[14]. Amazon. October, 2010). Amazon EC2 SLA. Available: http://aws.amazon.com/ec2-sla/