Volume 6, Issue 2, April 2019 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Cloud Computing Security Issues – A Survey

D. Naga Swetha
Assistant Professor
Department of Computer Science & Engineering
G. Narayanamma Institute of Technology and Science
Hyderabad, (T.S.) [INDIA]
Email: swetha@gnits.ac.in

ABSTRACT

Cloud computing is an emerging and propitious way for data storage and data transmission. Security and privacy becomes the most important concerns against the drastic development of cloud computing. The various approaches and techniques focusing on the data privacy and security on the data storage in the cloud are presented where the trustworthiness between the consumers and the cloud service providers are made. The data storage minimization and reduction in processing cost is essential for the any business, because data and information exploration is very noteworthy for making decisions. So the business organization assumes a durable trustworthiness between the business owners and the cloud service providers to transfer their data to the cloud. The security risks of cloud computing from the perspective of customer, service provider and government are discussed. Cloud computing security Enablers allows the users, services, servers, clouds, and any other entities to be predictable by systems and other parties.

Keywords:— *Cloud computing, Cloud computing Security Enablers, Security Issues, and Security Strategies.*

I. INTRODUCTION

Cloud Computing is a transformative computing paradigm that involves delivering applications and services over the Internet. It involves provisioning of computing, networking and storage resources on demand and providing these resources as metered services to the users. *NIST defines Cloud Computing as a model for* enabling *ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].*

The *main characteristics* of Cloud Computing includes – On-demand self service, Broad Network access, Resource Pooling, Rapid Elasticity, Measured Service, Performance, Reduced Costs, Outsourced Management, Reliability, Multi -tenancy (Virtual and Organic).

Cloud Service Models: The Cloud Computing model has three service delivery models[1].

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. Sales Force CRM is an example of the SaaS provider[1].

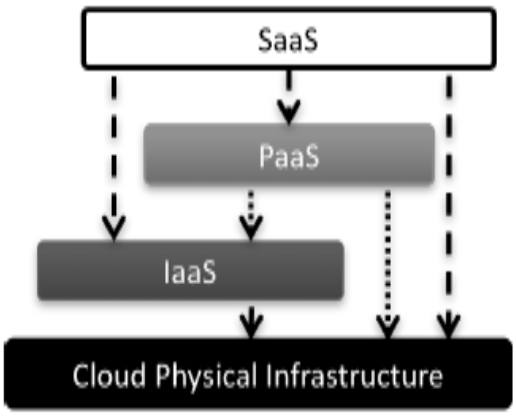

Figure 1: *Cloud Service Delivery models*

Cloud Deployment Models: There are four different deployment models of cloud computing. They are Public cloud, Community cloud, Hybrid cloud and Private cloud[3].

Public Cloud: A public cloud, or external cloud, is the most common form of cloud computing, in which services are made available to the general public in a pay-as-you-go manner.

Private Cloud: A Private Cloud, or internal cloud, is used when the cloud infrastructure, proprietary network or data centre, is operated solely for a business or organization, and serves customers within the business fire-wall.

Hybrid Cloud: A composition of the two types (private and public) is called a Hybrid Cloud, where a private cloud is able to maintain high services availability by scaling up their system with externally provisioned resources from a public cloud when there are rapid workload fluctuations or hardware failures.

Community Cloud: The idea of a Community Cloud is derived from the Grid Computing and Volunteer Computing paradigms. In a community cloud, several enterprises with similar requirement can share their infrastructures, thus increasing their scale while sharing the cost[4].

SECURITY ISSUES IN CLOUD COMPUTING

In this paper it is analysed about existing challenges and issues involved in the cloud computing security problem. The objective here is to identify the weak points in the cloud model. This analysis could help cloud providers and security vendors to have a better understanding of the problem. It also helps researchers being aware of the existing problem dimensions and gaps[2].

From *the cloud consumers' perspective,* security is the major concern that obstructs the adoption of the cloud computing model because:

(i) Enterprises outsource security management to a third party that hosts their IT assets (loss of control).

(ii) Co-existence of assets of different tenants in the same location and using the same instance of the service while being unaware of the strength of security controls used.

i. The lack of security guarantees in the SLAs between the cloud consumers and the cloud providers.

ii. Hosting this set of valuable assets on publicly available infrastructure increases the probability of attacks.

From the cloud providers' perspective, security requires a lot of expenditures (security solutions' licenses), resources (security is a resource consuming task). But skipping security from the cloud computing model roadmap will violate the expected revenues. So cloud providers have to understand consumers' concerns and seek out new security solutions that resolve such concerns[2].

The common security issue of cloud computing:

Seven Security *Issues of Cloud Computing Respectively by CSA and Gartner* Cloud Security Alliance (CSA) has published a white paper titled *Top Threats to Cloud Computing* by summarizing various security concerns of cloud computing. In this white paper, CSA has described seven security risks of cloud computing:

1) abuse and nefarious *use of cloud,*

2) *insecure interfaces and APIs*

3) malicious *insiders*

4) *shared technology issues*

5) *data loss or leakage*

6) *account or service hijacking*

7) *unknown risk profile[4].*

Gartner, a global authoritative IT research and analyst firm, has made a widespread investigation, and summarized seven security risks of cloud computing:

1) p*rivileged* user *access*

2) r*egulatory compliance*

3) d*ata location*

4) d*ata segregation*

5) r*ecovery*

6) *investigative support*

7) l*ong-term viability*.

Three Parties' Security Issues of Cloud Computing:

We analyze the security risks of cloud computing from the perspective of customer, service provider and government as follows[5].

The security risks confronted by customers: The security risks that customers need to confront in cloud computing environment include:

1) The downtime of cloud computing environment that brings great depress to the confidence of customers cannot be avoided totally

2) The leak of commercial secrets that means a nightmare for customer cannot be avoided totally

3) How to face the privilege status of cloud service provider and the security concerns such as fault elimination, damage compensation and business migration etc.

The security risks confronted by service providers: The security risks that service providers need to confront in cloud computing environment include:

1) How to assure the long-term secure operation of the cloud data center and isolate the fault to reduce its influence to a smallest extent are the security risks that service providers have to face with

2) How to fight against the numerous and aggressive network hackers is a disturbing security problem

3) For customers with various demands, how to effectively and securely manage these customers and identify and block the malicious customers is another unavoidable task.

The security risks confronted by government: The security risks that government administrators need to confront in cloud computing environment include:

1) How to enhance the security protection of a mass-scale data center is one important concern;

2) How to securely manage the numerous and various scale cloud service providers;

3) How to evaluate and rank the security level of cloud service providers and the security credit of cloud customers, and publish the proactive alarm of malicious programs.

III. Some Security Strategies of Cloud Computing

Security strategies w.r.t. security risks of cloud computing are as given below:

3.1 Securely Construction Strategies of Cloud Computing:

(a) ***Traditional Security Practice Mechanism:*** Traditional security practice such as the security protection of physical facilities, network, computer system, software application, and data still work in a cloud environment, and constructing a cloud environment should obey the common international information security standards such as ISO27001. Therefore, the traditional security practice mechanisms should be guaranteed for a secure cloud environment[7].

(b) ***Virtualization Security Risks Assessment:*** Irrespective of a public or private cloud, the construction and deployment of a cloud environment cannot lack numerous virtualization products. Hence, we need to consider the merits and drawbacks and security level of various virtualization technology resolutions and choose ***the*** best one to reduce the security risks brought by virtualization[11].

(c) ***Development Outsourcing Risk Control:*** Constructing a cloud environment is a large-scale systematic engineering with heavy work load and many advanced technologies, so it is hard to take charge of all development work for an organization. A practical action is to handover partial development work to several outsourcing parties, which will introduce some security risks. Therefore, we should identify the security risks incurred by outsourcing service and establish strict control strategies to assure their quality level and security requirement.

(d) ***Portability and Interoperability:*** Customers must keep in mind that they may have to change service providers for the sake of unacceptable cost increase at contract renewal time, business operations ceasing by service providers, partial cloud service closure without migration plans, unacceptable service quality decrease, and business dispute between cloud customer and provider etc. Therefore, portability and interoperability should be considered up front as part of the risk management and security assurance of any cloud program.

3.2. Securely Operation Strategies of Cloud Computing:

(a) ***Business Continuity Assurance:*** Rapid change and lacking transparency within cloud computing requires that business continuity plan and disaster recovery expertise be continuously engaged in monitoring the chosen cloud service providers. Regular inspections of a cloud service provider about cloud infrastructure and its physical interdependencies, disaster recovery and business continuity plans, contract documentation about security control action, recovery time objectives (RTOs), and access to data should be performed[6].

(b) ***Attack Proactive Alerting:*** Security incidents will be inevitable during in a cloud environment's operation. As cloud is an ultra-larger-scale distributed network system that contains a lot of physical infrastructure, host system, and business application, the range attacked by malicious people is very widespread and traditional attack proactive alerting mechanisms in small network environment may fail to work. Therefore, *how to monitor the network access all the time and alert timely on the malicious intrusion should be resolved.*

(c) ***Data Leak Prevention:*** Sensitive data leak is an important security risk of cloud environment. There are two potential data leaking ways: static data leakage and dynamic data leakage. Static data leakage means that the data stored in data center, application memory and terminal memory is accessed and leaked by unauthorized users, dynamic data leakage means that the data being transformed in cloud environment is accessed and leaked by customer account hijacking or network channel wiretapping. Therefore, all static and dynamic data are facing the security risk of leakage and tamper, and how to resolve it should be concerned seriously[10].

(d) ***Security Accident Notification & Response:*** Once security incidents occurred in a cloud environment, cloud service providers should notify their customers at first time, so that the customers can evaluate the potential damage done by these security incidents. Cloud service providers should start the emergency plan to response these security incidents, including application-level firewalls, proxies, application logging tools, disaster recovery project, and cloud service backup etc. Therefore, cloud service providers should create their respective standard security incident response mechanisms.

(e) ***Security Incidents Audit:*** To avoid the same security incidents occurring again, cloud service providers should find out the reasons of security incidents. Auditing can contribute to the reason analysis of security incidents in cloud environment. Traditional security auditing techniques such as security log, compliance check tools might not satisfy the auditing demand of cloud environment and so cloud service providers should develop some new security auditing approaches.

IV. Cloud Computing Security Enablers

A. Identity & Access Management (IAM) and Federation: Identity is a core of any security aware system. It allows the users, services, servers, clouds, and any other entities to be recognized by systems and

other parties. Identity consists of a set of information associated with a specific entity. This information is relevant based on context. Identity should not disclose user personal information "privacy". Cloud platforms should deliver or support a robust and consistent Identity management system. This system should cover all cloud objects and cloud users with corresponding identity context information. It should include: Identity Provisioning and de-provisioning, identity information privacy, identity linking, identity mapping, identity federation, identity attributes federation, single sign on, authentication and authorization. Such system should adopt existing standards, *such as SPML, SAML, OAuth, and XACML*, to securely federate identities among interacting entities within different domains and cloud platforms[8].

B. Key Management: Confidentiality is one of key objectives of the cloud computing security (CIA triad). Encryption is the main

Table 1: ***Shows the Different Types of Cloud Security Category***

S.No.	Category	Description
1	Security Standards	Defines the standards needed to take precautionary measures in the cloud computing so as to prevent attacks. It directs the policies of cloud computing for security without compromising reliability and performance.
2	Network	Consist of network attacks such as Denial of Service (DoS), Connection Availability, internet protocol vulnerabilities, DDoS, flooding attack, *etc*.
3	Access Control	Access control and Authentication and. It captures the issues that affect the privacy of user information and data storage.
4	Cloud Infrastructure	(a) Attacks that are strict to the cloud infrastructure (IaaS, PaaS and SaaS) such privileged insiders and tampered binaries
5	Data	(a) Data related security issues, including integrity, data migration, confidentiality, and data warehousing.

Table 2: Cloud Security Issues and Classifications

S.No.	Category	Issues
1	Security Standards	Absence of legal aspects (Service level agreement) Absence of security standards Compliance risks Trust Absence of auditing
2	Network	Network security configurations Appropriate installation of network firewalls Internet Dependence Internet protocol vulnerabilities
3	Access	Malicious insiders Service and Account and hijacking Privileged user access Browser Security Authentication mechanism
4	Cloud Infrastructure	(a) Quality of service (QoS) Sharing technical flaws Insecure interface of API Multi-tenancy Reliability of Providers Server Location and Backup Security Misconfiguration
5	Data	Data location Data loss and leakage Data redundancy Data privacy Data protection Data recovery Data availability

solution to the confidentiality objective, for data, processes and communications. Encryption algorithms either symmetric key -based or asymmetric are key-based. Both encryption approaches have a major problem related to encryption key management i.e. how to securely generate, store, access and exchange secrete keys. Moreover, PaaS requires application keys for all APIs and service calls from other applications. The applications' keys must be maintained securely along with all other credentials required by the application to be able to access such APIs.

C. Security Management: Based on the huge number of cloud stakeholders, the deep dependency stack, and the large number of security controls to deliver security requirements, the cloud security management becomes a more complicated research problem. Security management needs to include security requirements and policies specifications, security controls configurations according to the policies specified, and feedback from the environment and security controls to the security management and the cloud stakeholders[9].

D. Secure Software Development Lifecycle: The secure software development lifecycle (SDLC with security engineering activities) includes elicitation of the security requirements, threat modeling, augmentation of security requirements to the systems models and the generated code consequently. The cloud based applications will involve revolution in the lifecycles and tools used to build secure systems. The PaaS provides a set of reusable security enabling components to help developing secured cloud-based applications. Also security engineering of the cloud-based application should change to meet new security requirements imposed on such systems. Applications should support adaptive security (avoiding hardcoded security) to be able to meet vast range of consumers' security requirements. Adaptive application security is based on externalizing/delegating the security enforcement and applications security management to the cloud security management, cloud security services and security controls.

E. Security-Performance tradeoff optimization: The cloud computing model is based on providing services using SLAs. SLAs should cover objectives related to performance, reliability, and security. SLAs also define penalties that will be applied in case of SLA violation. Delivering high security level, *as one of SLA objectives*, means consuming much more resources that impact on the performance objective (the more adopted security tools and mechanism, the worst the impact on the performance of the underlying services). Cloud management should consider the trade-off between security and performance using utility functions for security and performance (least security unless stated otherwise). Moreover, we should focus on delivering adaptive security where security controls configurations are based on the current and expected threat level and considering other tradeoffs.

F. Federation of security among multi-clouds: When a consumer uses applications that depend on services from different clouds, he will need to maintain his security requirements enforced on both clouds and in between. The same case when multiple clouds integrate together to deliver a bigger pool of resources or integrated services, their security requirements needs to be federated and enforced on different involved cloud platforms.

V. CONCLUSION

The cloud computing model is one of the promising computing models for service

roviders, cloud providers and cloud consumers. But to best utilize the model we need to block the existing security holes.

The cloud security problems can be summarized as follows:

(i) Some of the security problems are inherited from the used technologies such as virtualization

(ii) 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).

(iii) Security management is very critical to control and manage this number of requirements and controls.

(iv) The cloud model should have a holistic security wrapper, such that any access to any object of the cloud platform should pass through security components first.

The cloud computing security solutions should:

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

(ii) Inherent in the cloud architecture and APIs should provide flexible security interfaces.

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

(iv) Support integration and coordination with other security controls at different layers to deliver integrated security.

(v) Be adaptive to meet continuous environment changes and stakeholders needs.

VI. Future Enhancements

To resolve cloud security management problem we need to:

(i) Capture different stakeholders security requirements from different perspectives and different levels of details

(ii) Map security requirements to the cloud architecture, security patterns and security enforcement mechanisms and

(iii) Deliver feedback about the current security status to the cloud providers and consumers.

Models will help in the problem abstraction and the capturing of security requirements of different stakeholders at different levels of details. Adaptiveness will help in delivering an integrated, dynamic and enforceable cloud security model. The feedback loop will measure the security status to help improving the current cloud security model and keeping cloud consumers aware with their asset's security status.

REFERENCES:

[1] D Naga Swetha, Asima Suman Qureshi, B Geetha Kumari, P Keerthi Chandrika, "Ensuring Interoperability in Generating and Integrating CDA for HIE based on Cloud Computing System" International Conference on Systems, Science, Control, Communication, Engineering and

Technology (2017): 21. Print.

[2] Mohamed Al Morsy, John Grundy and Ingo Müller, An Analysis of the Cloud Computing Security Problem, https://www.researchgate.net/ publication/307636677 September 2016.

[3] Sadhana Malgey, Mr. Pranay Chauhan A Review on Security Issues and their Impact on Cloud Computing Environment, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 6, June 2016.

[4] B. Rex Cyril, DR. S. Britto Ramesh Kumar Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey, International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 04 | July-2015.

[5] Varsha, Study of Security Issues in Cloud Computing, IJCSMC, Vol. 4, Issue. 6, June 2015, pp.230 – 234. Monjur Ahmed1 and Mohammad Ashraf Hossain, Cloud Computing and Security Issues in the Cloud, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[6] Dukaric, R. and Juric, M.B. (2013). Towards a unified taxonomy and architecture of cloud frameworks. Future Generation Computer Systems, 29, 1196–1210. doi:10.1016/ j.future.2012.09.006.

[7] Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysis and performance evaluation. Future Generation Computer Systems, 29, 387–401. doi:10.1016/ j.future.2011.08.008.

[8] Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ICCSEE.2012.193.

[9] Kim, J. and Hong, S. (2012). A Consolidated Authentication Model in Cloud Computing Environments. International Journal of Multimedia and Ubiquitous Engineering, 7(3), 151 -160.

[10] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616.

* * * * *