World Academy of Science, Engineering and Technology
International Journal of Humanities and Social Sciences
Vol:9, No:6, 2015

Classification of Attaks over Cloud Environment

Karim Abouelmehdi, Loubna Dali, Elmoutaoukkil Abdelmajid, Hoda Elsayed Eladnani Fatiha, Benihssane Abderahim

***Abstract*—**The security of cloud services is the concern of cloud service providers. In this paper, we will mention different classifications of cloud attacks referred by specialized organizations. Each agency has its classification of well-defined properties. The purpose is to present a high-level classification of current research in cloud computing security. This classification is organized around attack strategies and corresponding defenses.

***Keywords*—**Cloud computing, security, classification, risk.

I. Introduction

BEING new computing paradigm where the performance is through the Internet using a standard browser. Cloud computing builds on established trends that lower the cost of delivery of services meanwhile increases the speed and flexibility for better performance and deployment. [1]

Cloud computing incorporates virtualization, internet delivery of services, on-demand deployment, and open source software. The benefits of cloud computing are many. Such as pay for use service, the portability so the user can deploy it anywhere and anytime. In addition, free-up IT technicians who are responsible for updates, installing patches, etc. [2], [3].

II. Cloud Computing

Cloud computing is a general term for the delivery of hosted services over the Internet. Consuming compute resources as a utility - just like electricity - rather than having to build and maintain computing infrastructures in-house. Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches:

- On-demand self-service. A consumer can unilaterally provision computing capabilities as needed and automatically, without human interaction with a service provider.
- Broad network access. Computing capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, laptops, and PDAs) as well as other traditional or cloud-based software services.
- Resource pooling. A provider pools computing resources to serve several consumers using a multi-tenant model, which dynamically assigns and reassigns physical and virtual resources according to consumer demand. There is a degree of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources.
- Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in most cases automatically and rapidly released to scale out and scale in quickly. For a consumer, the capabilities appear to be unlimited and can be purchased in any quantity at any time.
- Measured service. Cloud systems automatically control and optimize resource usage by leveraging a metering capability according to the type of service. Usage can be monitored, controlled, and reported, providing transparency for both the provider and the consumer

III. Cloud Service Models

In general, clouds offer services at three different levels: IaaS, PaaS, and SaaS (Fig. 1). However, some providers can expose services at multiple levels [4]-[12].

- Software as a Service (SaaS) delivers software that is remotely accessible by consumers through the Internet with a usage-based pricing model. E.g., Live Mesh from Microsoft allows files and folders to be shared and synchronized across multiple devices.
- Platform as a Service (PaaS) offers a high-level integrated environment to build, test, and deploy custom applications as in Google's App Engine. Inside this layer resides the middleware system, a portable component for both grid and cloud systems. Examples include WSO2 Stratos, Windows Azure, and our middleware HIMAN.
- Infrastructure as a Service (IaaS) provisions hardware, software, and equipment to deliver software application environments with a resource usage-based pricing model. Infrastructure can scale up and down dynamically based on application resource needs. Typical examples are Amazon EC2 (Elastic Cloud Computing) Service, Eucalyptus, Microsoft Private Cloud.

IV. Deployment Model

In terms of Cloud deployment, there are four major types of Cloud Computing implementation called Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud (Fig. 2) [13]-[21].

Karim Abouelmehdi is with the Department of Computer Science, Laboratory LAMAPI, Chouaib doukali University Eljadida Morocco (e-mail: karim.abouelmehdi1@gmail.com).

Loubna Daliis with the Department of Computer Science, Bowie State University Maryland, USA (e-mail: Dalil0705@students.bowiestate.edu).

Abdelmajid Elmoutaoukkil is with the Department of Computer Science, Laboratory Laroseri, Chouaib doukali University Eljadida Morocco.

Dr. Hoda Elsayed is a Professor in Department of Computer Science and an IEEE Senior Member, Bowie State University Maryland, USA (e-mail: helsayed@bowiestate.edu).

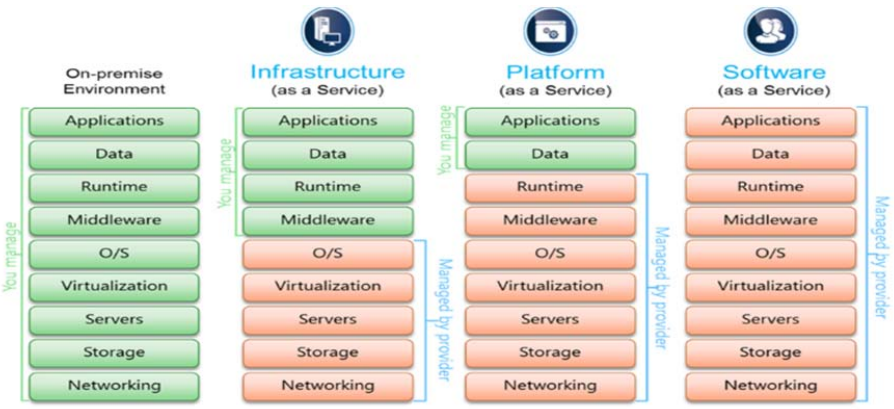

Fig. 1 Service Models of Cloud Computing

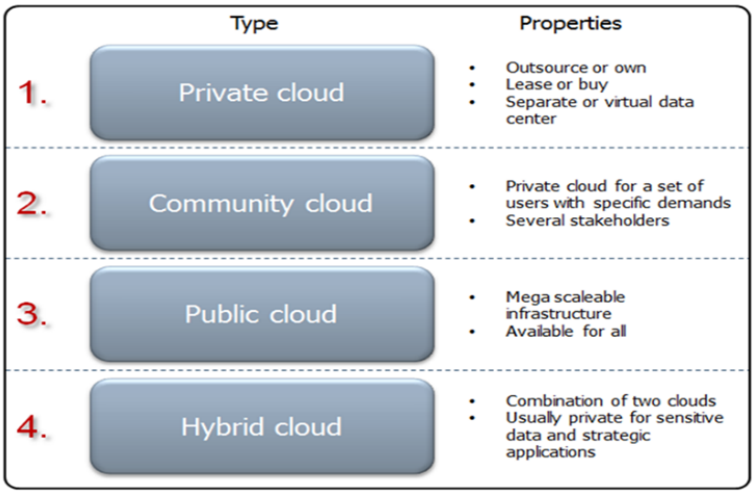

Fig. 2 Service Models of Cloud Computing

A. Private Cloud

A private cloud environment is often the first step for a corporation prior to adopting a public cloud initiative. Companies have discovered the benefits of consolidating shared services on virtualized hardware deployed from a primary data center to serve local and remote users.

B. Community Cloud

A community cloud is formed when several organizations with similar requirements share common infrastructure. The costs are spread over fewer users than a public cloud but more than a single tenant.

C. Public Cloud

Public cloud (off-site and remote) describes cloud computing where resources are dynamically provisioned on an on-demand, self-service basis over the Internet, via web applications/web services, open API, from a third-party provider who bills on a utility computing basis.

D. Hybrid Cloud

A hybrid cloud environment consists of some portion of computing resources on-site (on premise) and off-site (public cloud). Using public cloud services, so the users can leverage cloud solutions for specific functions that are too costly to maintain on-premise like disaster recovery of virtual server, test/development environments, and backups.

V. The Risks of Cloud Computing

First of all and before citing the existing classifications of attacks, we will start with the definition and classification of cloud risks.

The Committee of Sponsoring Organizations (COSO) of the Tread way Commission defined risk [22] as: “Risk is the possibility that an event will occur and adversely affect the achievement of the objectives." So, the risk analysis is an essential process to assess the impact of any dangerous condition or potential source of an adverse event. To be able to evaluate critically a risk of “harmful event”, we should classify the risk as either qualitatively or quantitatively [23].

The Quantitative risk can be expressed as a mathematical function. In cloud computing, the quality and amount of risk associated with a system or subsystem cannot have the same value of severity, occurrence and detection.

For example, in the SaaS environment, the entire system is managed by IT technicians and their interactions with machine

or systems, and if data integrity is compromised which might be caused by a software error Such as the man in the middle attack (external risk for both parties) or a malicious user input data (risk in the client Side).

The literature of the risk analysis showed that several techniques have been used and developed in different research area [23], [24] (engineering, chemistry, industry...) with different applications. Risk analysis and evaluation technique are classified into three main categories:

- Qualitative technique: Based on the analytical estimation process and security. This type uses calculations and simple procedures to achieve an acceptable level of risk and increase general awareness [22].
- Quantitative Technique: It can be estimated by the mathematical formula using historical data records and / or the expertise of experts in the field.
- Hybrid technique: A combination of both methods

VI. Related Work

A. The Risk Classification According to the Model CIA (Confidentiality, Integrity, Availability)

This classification model is established by several organizations such as GARNER [25], [26] (Table I).

B. Classification of Risks According to OWASP

According to [1], OWASP is a new type of organization that allows us to provide unbiased, practical and cost about the security of the application. OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. Like many projects open-source software, OWASP produces many types of materials in an open and collaborative manner. The OWASP Foundation is a non-profit entity that ensures the long-term success of the project.

The main goal of the project is to maintain a list of 10 security risks occurred within Cloud Computing and SaaS models. The community, cloud security experts and SaaS providers will be involved to maintain this list of risk.

Most risks are based on the assumption that the Cloud is a public or hybrid cloud.

C. Attacks OWASP

1. Accountability & Data Risk

The organization that chooses to use a public cloud to host its Business Service loses control of its data. This exposes them to severe risk of security that the organization must carefully consider and mitigate. They have to make sure that they do have the data recovery warranty, once the data entrusted to a third operator.

2. User Identity Federation

It is very important for businesses to maintain control over the identity of users who deploy services and applications from various cloud providers. Rather than allow cloud providers to create multiple identities that become too complex to manage. Users must be uniquely identifiable with federated authentication (e. g. SAML) that runs across cloud providers.

3. Regulatory Compliance

Data that is perceived to be secure in one country may not be perceived secure in another, because of the regulatory laws that vary from country and region to another. For example. The European Union has very strict privacy laws that may not comply with the data stored in The US.

4. Business Continuity and Resiliency

Business Continuity is an activity of an IT organization that ensures whether the business can be conducted in a disaster situation or not. In the case of an organization that uses cloud-based services, responsibility for business continuity is delegated to the cloud provider. This might create a risk to the organization not to have continuity of appropriate activities.

5. User Privacy and Secondary Usage of Data

Most of the social sites are vague on how they handle the personal data of users. In addition, most social sites work with default settings (least restrictive) to the user e.g. LinkedIn, Twitter, Facebook. It is easy to deduce the personal data of users, for this reason, the user has to make sure what data can/ cannot be used by their cloud providers.

6. Service and Data Integration

Organizations must ensure that their proprietary data is adequately protected when transferred between the end user and the cloud data center. The interception of data in transit should be a concern of each organization; the risk is much greater since data is transmitted over the Internet.

7. Multi-Tenancy and Physical Security

Multi- tenancy cloud means sharing resources and services across multiple clients (CPU, network, storage/database, Applications). It increases the dependency, the segregation and controls are needed to ensure that a tenant cannot deliberately interfere with the security (confidentiality, integrity, availability) of other tenants.

8. Incidence Analysis and Forensic Support

In the case of a security incident, applications and services hosted by a cloud provider are difficult to analyze, the logging can be distributed on multiple hosts and data centers that could be located in different countries and governed by different laws. Also, with the log files, the data belonging to multiple clients can be located on the same hardware and storage devices accordingly law enforcement agencies for legal recovery will be needed.

9. Infrastructure Security

The entire infrastructure must be securely configured, Applications, systems and networks must be built and configured with areas of prioritization, the security and the access have to be configured to allow only network protocols and the required applications. Also the administrative access should be granted. Regular risk assessments must be carried out, preferably by an independent third party.

10. Non-Production Environment Exposure

IT is an organization that develops in-house software applications using a set of non -production environments for the design, development and testing activities. If an organization uses a cloud provider for such a non - production environment. As a result, there is a high risk of unauthorized access, modification and stealing of data.

TABLE I
CLASSIFICATION OF RISKS ACCORDING TO THE MODEL OF THE CIA [25]-[28]

Threat	Description
Confidentiality	
Insider user threat: • Malicious cloud provider user • Malicious cloud customer user • Malicious third-party user (Supporting either the cloud provider or customer organizations)	The threat of insiders accessing customer data held within the cloud is greater as each of the delivery models can introduce the need for multiple internal users: SaaS Cloud customer and provider administrators PaaS application developers and test environment managers IaaS- third party platform consultants
External attacker threats: • Remote software attack of cloud infrastructure • Remote software attack of cloud applications • Remote hardware attack against the cloud • Remote software and hardware attack • Social engineering of cloud provider users, and cloud customer users	The threat from external attackers may be perceived to apply more to public Internet facing clouds, however all types of cloud delivery models are affected by external attackers, particularly in private clouds where user endpoints can be targeted. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups, with significant resources, attempting to retrieve data.
Data leakage: • Failure of security access rights across multiple domains • Failure of electronic and physical transport systems for cloud data and backups	A threat from widespread data leakage amongst many, potentially competitor organizations, using the same cloud provider could be caused by human error or faulty hardware that will lead to information compromise
Integrity	
Data segregation: • Incorrectly defined security perimeters • Incorrect configuration of virtual machines and hypervisors	The integrity of data within complex cloud hosting environments such as SaaS configured to share computing resource amongst customers could provide a threat against data integrity if system resources are effectively segregated
User access: • Poor identity and access management procedures	Poor access control procedures create many threat opportunities, for example, ex-employees of cloud provider maintain remote access to administer customer cloud services.
Data quality: • Introduction of faulty application or infrastructure components	The threat of data quality is increased as cloud providers host many customers' data. The introduction of a faulty or misconfigured component required by another cloud user could potentially impact the integrity of data for other cloud users sharing infrastructure
Availability	
Change management: • Customer penetration testing impacting other cloud customers • Infrastructure changes upon cloud provider, customer and third party systems impacting cloud customers	As the cloud provider has increasing responsibility for change management within all cloud delivery models, there is a threat that changes could introduce negative effects. These could be caused by software or hardware changes to existing cloud services
Denial of service threat: • Network bandwidth distributed denial of service • Network DNS denial of service • Application and data denial of service	The threat of denial of service against available cloud computing resource is generally an external threat against public cloud services. However, the threat can impact all cloud service models as external, and internal threat agents could introduce application or hardware components that cause a denial of service
Physical disruption • Disruption of cloud provider IT services through physical access • Disruption of cloud customer IT services through physical access • Disruption of third-party WAN providers services	The threat of disruption to cloud services caused by physical access is different between large cloud service providers and their customers. These providers should be experienced in securing large data center facilities and have considered resilience among other availability strategies. There is a threat that cloud user infrastructure can be physically disrupted more easily whether by insiders or externally where less secure office environments or remote working is standard practice.
Exploiting weak recovery procedures: • Invocation of inadequate disaster recovery or business continuity processes	The threat of inadequate recovery and incident management procedures being initiated is heightened when cloud users consider recovery of their own in-house systems in parallel with those managed by third-party cloud service providers. If these procedures are not tested, then the impact upon recovery time may be significant.

VII. CONCLUSION

These classifications of Cloud based risks that give a comprehensive vision of security to deploy a clear and strong strategy to minimize these risks, however they are not really relevant since the details and mechanisms of the attack are not explained. Consequently, we will offer a more objective classification to fit all possible attacks in our future work.

REFERENCES

[1] Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud computing and grid computing 360-degree compared. In: Grid Computing EnvironmentsWorkshop, pp. 1–10. IEEE (2008). DOI:10.1109/GCE.2008.4738445.

[2] Viega, J.: Cloud computing and the common man. Computer 42(8), 106–108 (2009). doi:10.1109/MC.2009.252.

[3] NIST: NIST Cloud Computing Program. http://www.nist.gov/itl/ cloud/ (2012). Accessed Sept. 2012.

[4] Banerjee, P., Friedrich, R., Bash, C., Goldsack, P., Huberman, B.,Manley, J., Patel, C., Ranganathan, P., Veitch, A.: Everything as aservice: powering the newinformation economy. Computer 44(3),36–43 (2011). doi:10.1109/MC.2011.67.

[5] Boampong, P.A., Wahsheh, L.A.: Different facets of security in the cloud. In: Proceedings of the 15th Communications and Networking Simulation Symposium, pp. 5:1–5:7. Society for Computer Simulation International, San Diego, CA, USA (2012).

[6] Gong, C., Liu, J., Zhang, Q., Chen, H., Gong, Z.: The characteristics of cloud computing. In: 39th International Conference on Parallel ProcessingWorkshop, pp. 275–279. IEEE Computer Society, Washington, DC, USA (2010). doi:10.1109/ICPPW.2010.45.

[7] Khorshed,M.T., Ali, A.S.,Wasimi, S.A.: A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener. Comput. Syst. 28(6), 833–851 (2012). doi:10.1016/j.future.2012.01.006.

[8] Lenk, A., Klems, M., Nimis, J., Tai, S., Sandholm, T.: What's inside the cloud? An architectural map of the cloud landscape. In: Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 23–31. IEEE Computer Society, Washington, DC, USA (2009). doi:10.1109/CLOUD. 2009.5071529.

[9] Patidar, S., Rane, D., Jain, P.: A survey paper on cloud computing. In: 2nd International Conference on Advanced Computing Communication Technologies, pp. 394–398. IEEE (2012). doi:10. 1109/ACCT.2012.15.

[10] Sadashiv, N., Kumar, S.: Cluster, grid and cloud computing: a detailed comparison. In: 6th International Conference on Computer Science Education, pp. 477–482. IEEE (2011). doi:10.1109/ ICCSE.2011.6028683.

[11] Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appli. 34(1), 1–11 (2011). doi:10.1016/j.jnca.2010.07.006.

[12] Xiao, Z., Xiao,Y.: Security and privacy in cloud computing. IEEE Commun. Surv. Tuts. 15(2), 843–859 (2013). doi:10.1109/SURV. 2012.060912.00182.

[13] Aguiar, E., Zhang, Y., Blanton, M.: An Overview of Issues andRecent Developments in Cloud Computing and Storage Security, pp. 1–31. Springer, Berlin (2013).

[14] Boampong, P.A., Wahsheh, L.A.: Different facets of security inthe cloud. In: Proceedings of the 15th Communications and Networking Simulation Symposium, pp. 5:1–5:7. Society for Computer Simulation International, San Diego, CA, USA (2012).

[15] Gul, I., Rehman, A., Islam, M.: Cloud computing security auditing.In: The 2nd International Conference on Next Generation Information Technology, pp. 143–148. IEEE (2011).

[16] Mohamed, E., Abdelkader, H., El-Etriby, S.: Enhanced data security model for cloud computing. In: 8th International Conference on Informatics and Systems, pp. CC-12–CC-17. IEEE (2012).

[17] Ramgovind, S., Eloff, M., Smith, E.: The management of security in cloud computing. In: Information Security for South Africa, pp. 1–7. IEEE (2010). doi:10.1109/ISSA.2010.5588290.

[18] Sabahi, F.: Cloud computing security threats and responses. In: IEEE 3rd International Conference on Communication Software and Networks, pp. 245–249. IEEE (2011). doi:10.1109/ICCSN. 2011.6014715.

[19] Songjie, Yao, J.,Wu, C.: Cloud computing and its key techniques. In: International Conference on Electronic and Mechanical Engineering and Information Technology, vol. 1, pp. 320–324. IEEE (2011).doi:10.1109/EMEIT.2011.6022935.

[20] Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appli. 34(1), 1–11 (2011). doi:10.1016/j.jnca.2010.07.006.

[21] Yang, J., Chen, Z.: Cloud computing research and security issues. In: International Conference on Computational Intelligence and Software Engineering, pp. 1–3. IEEE (2010). doi:10.1109/CISE. 2010.5677076.

[22] Enterprise Risk Management-Integrated Framework Executif Summary September 2004.Pdf

[23] H.J. Pasman, S. Jung, K. Prem, W.J. Rogers, X. Yang. Is Risk Analysis A Useful Tool For Improving Process Safety?. Journal Of Loss Prevention In The Process Industries 22 (2009) P. 769–777.

[24] P.K. Marhavilasa, D. Koulouriotisb, V.Gemenib. Risk Analysis And Assessment Methodologies In The Work Sites: On A Review, Classification And Comparative Study Of The Scientific Literature Of The Period 2000–2009. Journal Of Loss Prevention In The Process Industries Volume 24, Issue 5, September 2011, Pages 477–523.

[25] Ronald L. Krutz And Russell Dean Vines, Cloud Security. A Comprehensive Guide To Secure Cloud Computing.

[26] J.Heiser And Mark Nicolett: "Assessing The Security Risks Of Cloud Computing." Gartner, 3 June 2008 <Www.Gartner.Com/Displaydocument?Id=68 5308>Ages. SPIE.

[27] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 5.

[28] Peter Mell, Timothy Grance "The NIST Definition of Cloud Computing Special Publication 800-142"