IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2018

Addressing Security Challenges in Cloud Computing: A Review

Arundhati Nelli[1], Sushant Mangasuli[2], Jyothi Amboji[3]

Assistant Professor, Computer Science and Engineering, KLS Gogte Institute of Technology, Belagavi, India[1]

Assistant Professor, Computer Science and Engineering, Alva's Institute of Engg And Technology, Moodbidri, India[2]

Assistant Professor, Computer Science and Engineering, KLS Gogte Institute of Technology, Belagavi, India[3]

Abstract: Customers can opt for software and information technology services according to his requirements and can get these services on a leased basis from the network service provider and this has the facility to scale its requirements to up or down. This service is known as cloud computing, provided by the infrastructure provider which is a third party provider. Cloud computing provides many advantages to the customer like scalability, better economics of scaling, its ability to recover from problems , its ability to outsource non-core activities and flexibility. Cloud computing is a better option for the organizations to take as their best option without any initial investment and day by day frequent and heavy use of cloud computing is increasing but despite all the benefits a cloud offers to an organization there are certain doubts and threats regarding the security issues associated with a cloud computing platform. The security issues primarily involve the external control over organizational structure and management and personal and private data of the organization can be compromised. Personal and private data in this computing environment has a very high risk of breach of confidentiality, integrity and availability. Growth of cloud computing is mainly hampered due to these security concerns and challenges. This detailed study discusses about some of the security challenges associated with cloud computing services.

Keywords: Cloud Computing, Cloud Cryptography, Cloud CIA, Computer Network, Security Threats.

I. INTRODUCTION

The term "Cloud" is a meteorological metaphor associated with the representation of the internet, and which refers to the informal and fluid character of the latter. The term "Computing" has a double meaning in English: both programming (or computing) in one hand, but also computer science in general in the other hand. The term "cloud computing" represents the evolution of distributed computing through the network recently called emerging applications of internet: search engines and social networks. It is also the evolution of a more recent concept that has more to do with the second meaning of the word, the so-called computer "On-Demand". Cloud computing is a new technology enabling the provision of on-demand applications, services and IT infrastructure on demand accessed on the web. The cloud does not have yet a generally accepted definition, but according to the National Institute of Standards and Technology (NIST)[1], that: "This is a model for the infrastructure relocation". Offering a set of free web computing services like Email, online games and encyclopedia[2]. The cloud is characterized by availability, flexibility, scalability, pooling and payment for use. This technology uses web servers scattered around the world placed in secure data centers for storing customer data.
Cloud relieves the user of the overhead of physical installation and maintenance of her system, which automatically reduces the overall cost and enhances the system efficiency. Embracement of Cloud based services results in introduction of an abstraction layer between the physical storage or servers and the user whose data or services are being processed in the Cloud. The present scenario is such that the Cloud consumer who can be the data or service owner has to rely completely on the Cloud Service Provider (CSP) for the privacy and security of her information. The notion of mutual trust is achieved to some extent by negotiating the SLA but still a good number of cloud specific security issues become inevitable that need to be handled by either the CSP or the user itself [3].

Data holds the topmost position when it comes to IT security concerns, irrespective of the infrastructure being used. Cloud Computing is no exception to this, moreover it focuses on added security concerns because of its distributed nature and multi-tenant architecture. The data life cycle comprises its generation, storage, usage, distribution and destruction. Each CSP should support all these phases in the data life cycle with appropriate security mechanisms. For example, if the web application (shared application) is insecurely programmed, a customer could possibly use an SQL injection to gain unauthorized access to another customer's data, and delete or manipulate it. To prevent this, appropriate security measures must be implemented. The phenomenon of data deletion is again somewhat crucial in the cloud and therefore should be handled carefully by the CSP to ensure permanent and complete destruction of data on a

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2018

client's request. Moreover, the data backups (scope, saving intervals, saving times, storage duration, etc.) used to avoid data losses should be transparent and auditable for the customers. All these issues and several others need to be taken care of while using a cloud service.

II. CLOUD MODELS

A. Cloud Service Model

Cloud is classified into three service models that provide services at different layers of a business model.

• Software as a Service (SaaS): It describes a cloud service where consumers are able to access software applications running on a cloud infrastructure, over the internet. SaaS not only incurs no initial setup cost or underlying infrastructure maintenance cost but also automates all the updates. SaaS has the minimum customer control on security as the underlying infrastructure.

• Platform as a Service (PaaS): Platform as a Service (PaaS) is an abstracted and integrated cloud-based computing environment that supports the development, running, and management of applications. It is a delivery of a computing platform over the web. Control on the underlying cloud infrastructure including network, servers, operating systems, or storage, lies within the hands of the CSP whereas consumers are allowed to have certain controls over the deployed applications and possibly configuration settings for the application-hosting environment. It offers greater extensibility and greater customer control on security than SaaS.

• Infrastructure as a Service (IaaS): IaaS is the virtual delivery of computing resources in the form of hardware, networking, and storage services. In this model customer control spans the spheres of operating system, deployed services, and selected parts of the network. The infrastructure is managed wholly by the CSP. Thus it provides an increased amount of security control in the client's court.

B. Cloud Deployment Model

Cloud is classified into four deployment models that provide services to the people.

• Public Cloud: Public clouds are the most common way of deploying cloud computing. The cloud resources (like servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. In a public cloud, you share the same hardware, storage and network devices with other organisations or cloud "tenants." You access services and manage your account using a web browser. Public cloud deployments are frequently used to provide web-based email, online office applications, storage and testing and development environments.

• Private Cloud: A private cloud consists of computing resources used exclusively by one business or organisation. The private cloud can be physically located at your organisation's on-site data enter or it can be hosted by a third-party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organisation. In this way, a private cloud can make it easier for an organisation to customise its resources to meet specific IT requirements. Private clouds are often used by government agencies, financial institutions, any other mid- to large-size organisations with business-critical operations seeking enhanced control over their environment.

• Community Cloud:A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. This is controlled and used by a group of organizations that have shared interest. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

• Hybrid Cloud: Often called "the best of both worlds," hybrid clouds combine on-premises infrastructure, or private clouds, with public clouds so organisations can reap the advantages of both. In a hybrid cloud, data and applications can move between private and public clouds for greater flexibility and more deployment options. For instance, you can use the public cloud for high-volume, lower-security needs such as web-based email and the private cloud (or other on-premises infrastructure) for sensitive, business-critical operations like financial reporting. In a hybrid cloud, "cloud bursting" is also an option. This is when an application or resource runs in the private cloud until there is a spike in demand (such as seasonal event like online shopping or tax filing), at which point the organisation can "burst through" to the public cloud to tap into additional computing resources.

III.CLOUD SECURITY ISSUES

Trusting the Cloud Service Provider (CSP) and their offerings is one of the strongest driving forces behind the decision of a user to move into a cloud system or continue with the legacy system. Trust is based on the assessment as to

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2018

whether a provider has covered all the risks, including areas of data security, VM security as well as other government and compliance issues. The three factors that have been considered here for the evaluation of the Cloud system security are Confidentiality, Integrity, and Availability (CIA). As the CIA, domain is a widely used convention for determining the security concerns of a traditional information system, the main focus of this section is to generalize the security requirements in an existing Cloud system under this domain.

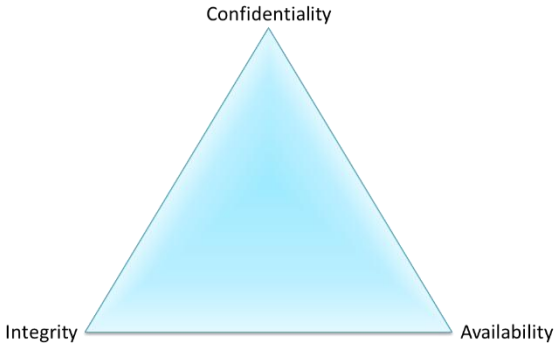

Fig 1. Cloud Security Pyramid

A. Confidentiality

Confidentiality is one of the five pillars of Information Assurance (IA). The other four are authentication, availability, integrity and no repudiation. Sensitive information or data should be disclosed to authorize users only. In IA, confidentiality is enforced in a classification system. For example, a U.S. government or military worker must obtain a certain clearance level, depending on a position's data requirements, such as, classified, secret or top secret. Those with secret clearances cannot access top secret information.

Best practices used to ensure confidentiality are as follows:

- An authentication process, which ensures that authorized users are assigned confidential user identification and passwords. Another type of authentication is biometrics.
- Role-based security methods may be employed to ensure user or viewer authorization. For example, data access levels may be assigned to specified department staff.
- Access controls ensure that user actions remain within their roles. For example, if a user is authorized to read but not write data, defined system controls may be integrated.

The following table shows examples of confidentiality breaches. No health care-related or credit card data is accessed in these breaches. The person making the breach would not have access to this data in the normal scope of the person's job.

TABLE 1 Source of Confidentiality

Source and Intent of Confidentiality Breach	Accidental	Purposeful
Internal	An employee accidentally opens the wrong file and sees the performance review of a colleague.	An employee seeks out the online purchase records of a friend or celebrity.
External	A website visitor mistypes a web page address and gains access to an unpublished area of the website that contains a list of online discount codes that isn't publicly available.	A hacker gains access to the email system and all inbound and outbound email history for all of the nonprofit's staff.

Cloud security has both technical and procedural aspects that are often taken care of by the cloud service provider's information security infrastructure. Cloud service providers often engage information security professionals, so they usually have much stronger information security capabilities than you, their customer. However, breakdowns in cloud security usually occur with the customer rather than the service provider. Certain technical and procedural aspects rely on proper configuration and training by the organization.

B. Integrity

Data that is stored in the cloud could suffer from the damage on transmitting to/from cloud data storage. Since the data and computation are outsourced to a remote server, the data integrity should be maintained and checked constantly in order to prove that data and computation are intact. Data integrity means data should be kept from unauthorized modification. Any modification to the data should be detected. Computation integrity means that program execution should be as expected and be kept from malware, an insider, or a malicious user that could change the program

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2018

execution and render an incorrect result. Any deviation from normal computation should be detected. Integrity should be checked at the data level and computation level. Data integrity could help in getting lost data or notifying if there is data manipulation.

To maintain integrity, data must not be changed in transit and steps must be taken to ensure that data cannot be altered by an unauthorized person or program. Such measures include implementing user access controls and version control to prevent erroneous changes or accidental deletion by authorized users. Other measures include the use of checksums and cryptographic checksums to verify integrity. Network administration measures to ensure data integrity include documenting system administration procedures, parameters and maintenance activities, and creating disaster recovery plans for occurrences such as power outages, server failure or security attacks. Should data become corrupted, backups or redundancies must be available to restore the affected data to its correct state.

Measures must also be taken to ensure integrity by controlling the physical environment of networked terminals and servers because data consistency, accuracy and trustworthiness can also be threatened by environmental hazards such as heat, dust or electrical problems. Some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Practices followed to protect data integrity in the physical environment include keeping transmission media (such as cables and connectors) covered and protected to ensure that they cannot be tapped, and protecting hardware and storage media from power surges, electrostatic discharges and magnetism.

C. Availability

Availability is one of the main pillars of Information Assurance (IA). When a system is regularly non-functioning, information availability is affected and significantly impacts users. In addition, when data is not secured and easily available, information security is affected, i.e., top secret security clearances. Another factor affecting availability is time. If a computer system cannot deliver information efficiently, then availability is compromised. Data availability must be ensured by storage, which may be local or at an offsite facility. In the case of an offsite facility, an established business continuity plan should state the availability of this data when onsite data is not available. At all times, information must be available to those with clearance.

Denial of Service attack in the Cloud system is one of the major causes of service or data unavailability. The attacker generally sends huge amount of vague requests to a certain service. When the Cloud Computing operating system notices the high workload on the flooded service, it starts providing more computational power (more service instances) to handle the additional workload. Indirect Denial of Service attack is also possible in a Cloud system where other services running with a flooded service on the same server may also become unavailable. Once the server's hardware resources are exhausted after processing the flooding attack requests, the other service instances on the same hardware machine may automatically fail to perform their intended tasks. At last Natural disasters like fire, flood etc. in a data center is likely to affect both the primary and redundant copies of data. Therefore availability is once more threatened here and effective measures should be taken to cope up with these situations.

IV. CONCLUSION

The paper covers the essential security loop holes as well as security requirements of an existing Cloud system. Generalized view of these issues have been presented here to enhance the importance of understanding the security flaws of the Cloud computing framework and devising suitable countermeasures for them. Finally, various cloud security schemes have been discussed on a comparative framework. On a whole, the paper aims at constructing a proper snapshot of the present scenario and future prospects of Cloud security.

REFERENCES

[1] 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(6): 599-616, doi:10.1016/j.future.2008.12.001

[2] Mell P.M. and Grance.T. 2011. "The NIST Definition of Cloud Computing." In Computer Security Publications from the National Institute of Standards and Technology (NIST) SP 800145.Gaithersburg: National Institute of Standards & Technology.

[3] Chen D and Zhao H, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 International Conference on ComputerScience and Electronics Engineering, Hangzhou, 2012, pp. 647-651.

[4] Wu H, Ding Y, Winer C and Yao L, "Network security for virtual machine in cloud computing," 5th International Conference on Computer Sciences and Convergence Information Technology, Seoul,2010, pp. 18-21.

[5] Xiong D., Zou P., Cai J., He J. (2015) A Dynamic Multi-domain Access Control Model in Cloud Computing. In: Abawajy J., Mukherjea S., Thampi S., Ruiz-Martínez A. (eds) Security in Computing and Communications. SSCC 2015. Communications in Computer and Information Science, vol 536. Springer, Cham

[6] S. Sethi and S. Sruti, "Cloud security issues and challenges," Resource Management and Efficiency in Cloud Computing Environments, p. 89, 2016.

[7] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio, "Security issues in cloud environments: a survey,"International Journal of Information Security, vol. 13, no. 2, pp. 113–170, 2014.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2018

[8] S. Kuila, S. Shridhar, C. Patel, and N. C. S. Iyengar, "Cloud computing security by using mobile otp and an encryption algorithm for hospitalmanagement," Journal of Computer and Mathematical Sciences, vol. 7, no. 11, pp. 558–565, 2016.
[9] I. El Mir, D. S. Kim, and A. Haqiq, "Security modeling and analysis of an intrusion tolerant cloud data center," in Complex Systems (WCCS),2015 Third World Conference on. IEEE, 2015, pp. 1–6.
[10] Hwang K, Li D. Trusted cloud computing with secure resources and data coloring. IEEE Internet Computing. 2010 Sep;14(5):14-22.
[11] Tian L.Q, Lin C and Ni Y, "Evaluation of user behavior trust in cloud computing," 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), Taiyuan, 2010, pp. V7-567-V7-572.

BIOGRAPHIES

Arundhati Nelli[1] working as Assistant Professor in KLS Gogte Institute of Technology, Belagavi, having an teaching experience of 8 years. My research interests are Cryptography and Security Systems, Cloud Computing, Wireless Sensor Networks, Mobile Computing.

Sushant Mangasuli[2] working as Assistant Professor in Alva's Institute of Engineering and Technology, Moodbidri, having an teaching experience of 8 years. My research interests are Cryptography and Security Systems, Cloud Computing, Wireless Ad-hoc Networks, Mobile Computing.

Jyothi Amboji[3] working as Assistant Professor in KLS Gogte Institute of Technology, Belagavi, having an teaching experience of 8 years. My research interests are Software Engineering, Cryptography and Security Systems, Cloud Computing.