International Journal of Research

International Journal of Research (IJR) e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, June 2015
Available at http://internationaljournalofresearch.org

Security Risks Associated with the Cloud Computing

G.Rajesh Babu[1]; G.Ananth Kumar[2] & Vishal Tiwari[3]

[123]*Assistant Professor, CSE Department,* TGPCET, Nagpur.
rajeshbabu.cse@tgpcet.com[1],ananthkumar.cse@tgpcet.com[2],vishal.cse@tgpcet.com

Abstract—
Security in distributed computing is developing as a sub space of PC security, data security and system security. Notwithstanding the security chances officially display in IT, distributed computing additionally incorporates dangers identified with protection, agreeability regulations, personality, utilization of virtual machines, security of information and the security of the system through which the information ventures. This paper examines these security dangers connected with distributed computing.

Keywords — cloud computing; security; cloud security; information; data

I. INTRODUCTION

Distributed computing can be characterized as an approach to upgrade registering administrations by empowering clients to get to programming applications and processing administrations which are put away off-site at areas as opposed to the associations neighborhood datacenter or the client's desktop

[1]. Countless administrations are given over the web and the clients pay just for the administrations they devour. Distributed computing permits an endeavor to demand IT benefits without needing to spend a lot of cash to buy, send and deal with the assets at their nearby destinations [2].

Case in point, if an organization concludes that it needs to build its capacity by a few terabytes, it essentially pays for the administration for the given limit and it can get to the information from diverse areas. There is no requirement for the association to buy and execute the capacity foundation themselves.

Distributed computing can be isolated into three zones [3]:

1) Software as a Service (SaaS): The ability gave to shoppers permits them to utilize a product supplier's applications running in the cloud utilizing a slender customer, for example, a program over the web. For instance, Google Apps permits associations to get to Google's administrations, for example, Gmail, Google Groups, Google Calendar, and so on utilizing their own area name.

2) Platform as a Service (Paas): The ability gave to the customers permits them to convey applications to the cloud which they create themselves. Case in point, the Google App Engine permits engineers to make applications and afterward send those applications to Google's cloud.

3) Infrastructure as a Service (IaaS): The ability gave to customers permits them to get to the supplier's computational and stockpiling base in a unified administration. For instance, Amazon Web Services gave by Amazon.com permits an association to utilize various Amazon.com's remote processing administrations.

Distributed computing disentangles the security dangers for various little and medium ventures as these associations don't have the assets to put resources into data security. Accordingly, these associations think that it helpful and less expensive to outsource security to the cloud administration suppliers, for example, Microsoft, Google and Amazon.com. Nonetheless, some medium and extensive ventures have made huge interests in their own data security and need to conform to the regulations of diverse nations [9]. There are various security dangers for these associations as they move into the cloud and these are examined in point of interest in this paper.

II. THE CIA TRIAD

The three center standards of data security are privacy, trustworthiness and accessibility – known as the CIA triad. All the data security controls, shields, dangers, vulnerabilities and security forms for each association are liable to the CIA triad [9].

A. Privacy

Privacy is the aversion of unapproved divulgence of data. Secrecy is guaranteed by: system security conventions, system validation administration and information encryption administrations.

B. Trustworthiness

Trustworthiness is the surety that the message that is sent is the same as the message got and that the message is not changed in travel. Uprightness is ruptured if the transmitted information is modified when it is in travel. Honesty is guaranteed by: Firewall administrations, correspondence security and interruption discovery.

C. Accessibility

Accessibility is the certification that data will be accessible to the shopper in an auspicious and continuous way when it is required paying little respect to area of the client. This implies that the cloud foundation, the security controls, and the systems joining the customers and the cloud framework ought to dependably be working accurately. Accessibility is guaranteed by: adaptation to internal failure, validation and system security

III. PRIVACY

Privacy is a fundamental human right and is defined as —an individual’s right to be left alone_. The right to privacy is enshrined in the United Nations Declaration of Human Rights and also the European Union Convention on Human Rights [5].

Cloud computing raises a number of legal issues related to privacy and information security. There are risks involved for individual users, enterprise users and also the providers of cloud services. These risks are summarized below [4][5][9]:

1) The risk of the users inadvertently giving away their personal information by posting the data to the cloud.
2) The risk that malware and viruses will be transmitted through security loopholes in the cloud service provider’s software.
3) The risk that the information stored in the cloud is used for unauthorized purposes such as advertising.
4) Enterprise users of cloud services have to determine the data retention policies of the cloud service providers. They may need to delete all or part of the data from the clouds which may not be possible.
5) Enterprise users will also have to rely on the cloud service provider for logs of how information is accessed, copied, modified and used.
6) The risk for cloud service providers is that the information in the cloud may be used for purposes different than the original cloud service intention.

IV. THREATS TO INFRASTRUCTURE AND DATA

A threat is simply a possibility that a system may have security vulnerabilities which may be exploited to cause damage to the system. Threats may be malicious or accidental, but if realized, they may cause an irreparable loss of confidentiality, integrity or availability. The threats to the cloud service provider’s infrastructure and data are summarized below [6][7][8][9]:

1) Authentication: The risk associated with unauthorized authentication is that users may be able to access cloud services at a higher level than what they are assigned.
2) Inappropriate use of System Infrastructure:

   The risk is that authorized users of a company’s network may use the network for non-business uses such as inappropriate web browsing. This may result in litigation accusing employers and cloud service providers of employee harassment.
3) Eavesdropping: The risk is that the communication channels between the users and the cloud service providers may be monitored by unauthorized parties. Certain network transmission methods such as wireless and mobile communications are especially susceptible to eavesdropping.
4) Network Intrusion: The risk is that an external source may exploit the security vulnerabilities in the cloud service provider’s software and access the user’s data.
5) Denial of Service Attacks: The risk is that external users may try to launch a denial-of-service attack on the cloud service provider’s network to try and make their computer resources unavailable to corporate and individual users.
6) Session hijacking: This is a method of taking over a legitimate session between a client and server obtaining the session ID and then posing as the user. The attacker is then able to do everything that the user is authorized to do on the network.

V. VIRTUALIZATION RISKS

Virtualization is the ability to run multiple operating systems on a single physical system and share the underlying hardware resources. Cloud computing relies heavily on virtualized systems and this introduces a number of risks which are identified below [6][9]:

1) Complex configuration: Virtual systems are much more complex as they add several layers of networks and systems. This increases the possibility of creating security vulnerabilities through improper configuration of virtual machines.

2) Privilege escalation: It is possible for a hacker to access a virtual machine with a lower level of access rights and then leverage the machine to attack a machine with a higher level of access rights using a hypervisor.

3) Inactive virtual machines: It is possible for dormant virtual machines to store sensitive data and this creates security risks if the machine is improperly accessed.

4) Poor access controls: A hypervisor facilitates access to all virtual machines and it may expose a trusted network through deficient patching, poor monitoring tools and poorly designed access control systems.

VI. CONCLUSION

Cloud computing is an emerging frontier in the field of Information Technology. It brings the promise of convenience, elasticity, transparency and economy. However, there are a number of security risks associated with these benefits. Enterprises will have to understand the risks associated with cloud computing and also have an understanding of the laws, regulations and best practices to ensure that they choose the proper cloud service provider.

Security in cloud computing is a shared responsibility between the IT department of an enterprise and the cloud service provider. Therefore, even when IT infrastructure can be moved into the cloud, the responsibility for information security cannot be entirely outsourced to the cloud service provider.

REFERENCES

[1] B. Grobauer, T. Walloschek and E. Stöcker, "*Understanding Cloud-Computing Vulnerabilities*", IEEE Security and Privacy, 10 Jun. 2010.

[2] K.Dahbur, B.Mohammad, A.B.Tarakji, —*A survey of risks, threats and vulnerabilities in cloud computing*_ in ISWSA '11 Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, 2011

[3] M.Creeger, —Cloud Computing: An Overview_ in Distributed Computing, Vol. 7, No. 5, June 2009

[4] S.Pearson, *Taking account of privacy when designing cloud computing services*, in Software Engineering Challenges of Cloud Computing, 2009. CLOUD '09. ICSE Workshop on, May 2009, pp 44 – 52

[5] The Royal Academy of Engineering, —*Dilemmas of Privacy and Surveillance: Challenges of Technological Change*_, March 2007. Available : www.raeng.org.uk/policy/reports/default.htm

[6] F.Lombardi and R.D.Pietro, —Secure virtualization for cloud computing_ in Journal of Network and Computer Applications, Vol. 34, No. 4, July 2011.

[7] M.Yildiz, J.Abawajy, T.Ercan and A.Bernoth, —A Layered Security Approach for Cloud Computing Infrastructure_ in 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, December 2009

[8] G.Peterson, "*Don't Trust. And Verify: A Security Architecture Stack for the Cloud,*" IEEE Security and Privacy, vol. 8, no. 5, pp. 83-86, September 2010

[9] R.L.Krutz and R.D.Vines, —*Cloud Computing Software Security Fundamentals*_in Cloud Security: A Comprehensive Guide to Secure Cloud Computing_, New York City, NY, Wiley, 2010