Asian Journal of Convergence in Technology Volume II Issue III
Issn No.:2350-1146, I.F-2.71

A Review of Data Security in Cloud Computing

Akshata Anand Parab
Department of MCA
Finolex Academy of Management and Technology. Ratnagiri.

Abstract- Cloud computing is an emerging paradigm for large scale infrastructures. It has the advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-per-use business model. These new features have a direct impact on the IT budgeting but also affect traditional security, trust and privacy mechanisms. Cloud computing has many advantages such as flexibility, efficiency, scalability, integration, and capital reduction. Moreover, it provides an advanced virtual space for organizations to deploy their applications or run their operations. With disregard to the possible benefits of cloud computing services, the organizations are reluctant to invest in cloud computing mainly due to security concerns. Security is one of the main challenges that hinder the growth of cloud computing. In this paper we assess how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed.

Keywords- Cloud Computing, Security Issues, Data protection, Iaas, Paas, Saas

I. INTRODUCTION

Cloud computing is latest trend in IT world. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc.Concept of this new trend started from 1960 used by telecommunication companies until 1990 offered point to point data circuits and then offered virtual private networks. But due to network traffic and make network bandwidth more efficient introduced cloud to both servers and infrastructure. The development of this Amazon played vital role by making modern data centers. In 2007 Google, IBM and many remarkable universities and companies adopted it. And in 2008 Gartner highlighted its characteristics for customer as well service providers [1]. This paper gives a review of cloud computing and its security issues.

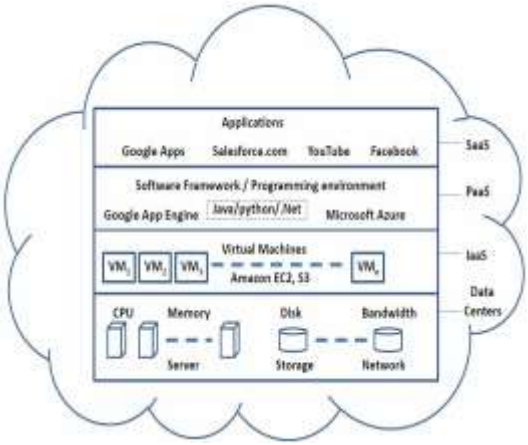

Figure 1. High Level View of Cloud Computing Architecture [2]

II. THREADS RELATED CLOUD COMPUTING

A. Cloud Confidentiality

Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes, or devices. Hence, we must make sure that the users' confidential data, which the users do not want to be accessed by service providers is not disclosed to service providers in the cloud computing systems, including applications, platforms, CPU and physical memories. It is noted that users' confidential data is disclosed to a service provider only if all of the following three conditions are satisfied simultaneously [3]:

Condition 1) the service provider knows where the users' confidential data is located in the cloud computing systems.

Condition 2) the service provider has the privilege to access and collect the users' confidential data in the cloud computing systems.

Condition 3) the service provider can understand the meaning of the users' data.

Computation tasks need to be kept confidential from both the service provider and other customers. Confidentiality remains as one of the greatest concerns with regards to cloud computing. This is because the customers outsource their data and computation tasks on cloud servers, which are controlled and managed by potentially untrustworthy cloud providers [4].Threats to cloud Confidentiality: Cross-VM attack via Side Channels, Malicious SysAdmin

B. Cloud Integrity

Similar to confidentiality, the notion of integrity in cloud computing concerns both data integrity and computation integrity. Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users, and that any incorrect computing will be detected.[5] Threats to Cloud Integrity: Data loss/manipulation, Dishonest computation in remote servers

C. Cloud Availability

Availability is crucial since the core function of cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system. In this section, we have studied two kinds of threats that impair cloud availability. Threats to Cloud Availability: Flooding Attack via Bandwidth Starvation, Fraudulent Resource Consumption (FRC) attack

D. Cloud Privacy

Privacy is yet another critical concern with regards to cloud computing due to the fact that customers' data and business logic reside among distrusted cloud servers, which are owned and maintained by the cloud provider. Therefore, there are potential risks that the confidential data (e.g., financial data, health record) or personal information (e.g., personal profile) is disclosed to public or business competitors. Privacy has been an issue of the highest priority [6], [7], [8]. Throughout this text, we regard privacy- preservability as the core attribute of privacy. A few security attributes directly or indirectly influence privacy preservability, including confidentiality, integrity, accountability, etc. Evidently, in order to keep private data from being disclosed, confidentiality becomes indispensable, and integrity ensures that data/computation is not corrupted, which somehow preserves privacy. Accountability, on the contrary, may undermine privacy due to the fact that the methods of achieving the two attributes usually conflict. Threats to Cloud Privacy: In some sense, privacy-preservability is a stricter form of confidentiality, due to the notion that they both prevent information leakage. Therefore, if cloud confidentiality is ever violated, privacy-preservability will also be violated. Similar to other security services, the meaning of cloud privacy is twofold: data privacy and computation privacy.

III. CLOUD COMPUTING ISSUES

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. These are the following concerning issues for the cloud computing [9] [10].

a. Security
b. Privacy
c. Reliability
d. Legal Issues
e. Open standard
f. Compliance
g. Freedom
h. Long-term Viability

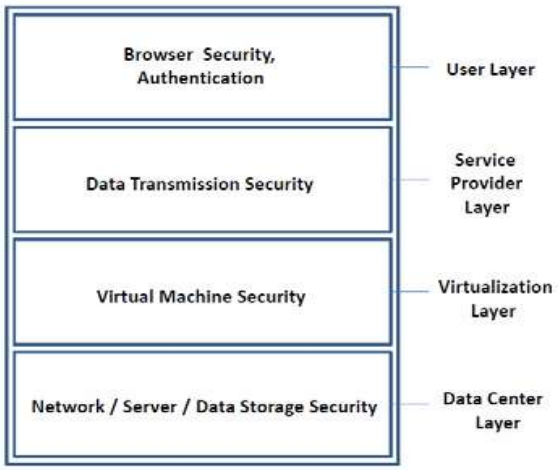

Figure 2. High Level Security Architecture of Cloud Computing [2]

IV. SOLUTION FOR EXISTING ISSUES

To advance cloud computing, the community must take proactive measures to ensure security. The solutions for the existing issues are the following [11].

a. Data encryption.
Before storing it at virtual location, encrypt the data with your own keys and make sure that a vendor is ready for security certifications and external audits.
b. Identity management.
c. Access control.
d. Reporting of security incidents, personnel and physical layer management should be evaluated.
e. You should minimize personal information sent to and stored in the cloud.
f. CSP should maximize the user control and provide feedback.

V. CONCLUSION

Every new technology has its pros and cons, similar is the case with cloud computing. Although cloud computing provides easy data storage and access. But there are several issues related to storing and managing data that is not controlled by owner of the data. This paper discussed security issues for cloud. These issues include cloud integrity, cloud confidentiality, cloud availability, cloud privacy. There are several threats to cloud confidentiality including cross-VM attack and malicious sysadmin. On the other hand integrity of cloud is compromised due to data
Loss and dishonest computation in remote servers. DoS (Denial of Service attack is the most prevent the data available to its intended users. The last issue is cloud privacy and it is similar to cloud confidentiality. if cloud confidentiality is at risk, cloud privacy will also be at risk.[5]

6. Future work-

Cloud computing is the most modern technology so lots of issues are remained to consider. It has many open issues some are technical that includes scalability, elasticity ,data handling mechanism, reliability, license software, ownership, performance, system development and management and non-technical issues like legalistic and economic aspect. Cloud computing still unknown "killer application" will establish so many challenges and solutions must develop to make this technology work in practice. So the research is not stop here much work can be done in future. The model presented in this paper is the initial step and needs more modifications; however it can provide the basis for the deeper research on security deployment of cloud computing for the research community working in the field of Cloud Computing.[12]

REFERENCES

[1] Janakiram MSV Cloud Computing Strategist; (2010), "Demystifying the Cloud An introduction to Cloud Computing", Version 1.0 – March.
[2]Cloud Computing: Security Issues and Research Challenges by Rabi Prasad Padhy[1] Manas Ranjan Patra[2] Suresh Chandra Satapathy[3]

[3] DoD Trusted Computer System Evaluation Criteria, http://csrc.nist.gov/publications/history/ dod85.pdf.

[4] Stephen S. Yau and Ho G. An "Confidentiality Protection in Cloud Computing Systems", Int J Software Informatics, Vol.4, No.4, December 2010, pp. 35-1365.

[5] Security Issues in Cloud Computing by Abhishek Goel1, Shikha Goel2

[6] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," IEEE
Commun. Surveys Tuts., DOI:10.1109/SURV.2011.122111.00145, in press.

[7] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and Privacy in RFID and Applications in Telemedicine," IEEE
Commun. Mag., Vol. 44. No.4, Apr. 2006, pp. 64-72.

[8] H. Chen, Y. Xiao, X. Hong, F. Hu, J. Xie, "A Survey of Anonymity in Wireless Communication Systems,"
(Wiley Journal) Security and Communication Networks, Vol. 2 No. 5, Sept./Oct., 2009, pp. 427-444.

[9] Jack Schofield. Wednesday 17 June 2009 22.00 BST, http://www.guardian.co.uk/technology/2009/jun/17/cloud-computingjack-schofield.

[10] Gartner. "Seven cloud-computing security risks". http://www.infoworld.com July 02,2008.

[11] Jianfeng Yang and Zhibin Chen, Cloud Computing Research and Security Issues, 2010 IEEE 978-1-4244-5392-4/10, 2010.

[12] A review on cloud computing security issues & challanges by F. A. Alvi1, Ψ, B.S Choudary2 ,N. Jaferry3 , E.Pathan4