Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on Security Analysis for Cloud Computing

Avinash Parihar, Deepali Chorage, Dhanshri Bichkule, Pooja Kumbhar
Computer Pune University, Pune, Maharashtra,
India

Abstract— Cloud computing is resilient, inexpensive platform for supplying business or customer IT services over the Internet. Cloud computing is somehow risky as the fundamental services are often outsourced to the third party, which make it difficult to maintain data security and privacy, backing data and service accessibility. Cloud computing prestige many technologies(SOA, virtualization), it also heirdom their security issues, which we discuss here, identifying the main insecurity in this kind of system and the most important thread found in the outfit relate to cloud computing and its environment as well as to identify relate insecurity and threat with possible solution.

Keywords— Prestige, Resilient, Heidom, Data security, Cloud Computing

I. INTRODUCTION

This Cloud computing is one of the most popular technology . It is one of the mickle, useful and famous technology now a days . It takes too much attention in the industrial and scientific co mmunity. It takes too much attention in the industrial and scientific community.

As per the Gartner's[1] study, cloud computing is first ranked technology from the top ten technologies and with a better expectation in successive years by organizations and companies.

Cloud computing enables omnipresent, essay, on demand network access to the networks, servers, storage, application, and services that can be quickly provisioned and emitted with minimum management assay or service supplier interaction

Cloud computing looks as computational paradigm as well as a distribution architecture and the main objective of cloud computing is to provide secure, rapid, easy data storage and net computing facility with all computing mediums conceives as service and released over a internet[2][3] .

The cloud enhanced co-operation, briskness, scalability, skill to adapt the undulation according to demand, accelerate development work and gives potential for reduction of cost through optimized and efficient computing[4][7]

II. METHODOLOGY

Methodological reviews of security issues for cloud Computing

Related to security in cloud computing, we have to carried out the methodological review of the present outfit not only in order to summarized the available vulnerabilities and threats about this topic but also to identify and analysed the current state and the most important security issue of cloud computing

Question formalization

The main focus of the question was to identify the most relevant issues in cloud computing which consider insecurity, threats, risk, requirement and solution of security for the cloud computing

The main question formed here was what security vulnerability and threats are the important in cloud computing which have to be studied in details with the purpose of handling them? The important word and related concepts that makes up this query and that were used during the execution are: secure cloud system, SaaS security, IaaS security, PaaS security, cloud threads, best practice in cloud.

Cloud Computing Security Issues

There are number of security issues in cloud computing as it bring many technologies such as networks, databases, operating system ,virtualization , resource management scheduling, transaction management , concurrency control, load balancing and memory management. Therefore security issues for lot of these systems and technologies are similar to cloud computing. For example, the networks that interconnect the systems in a cloud should be similar. Data security implicates encrypting the data as well as convincing that proper rules are enforced for data sharing. We can apply data mining technologies for malware detection in the cloud.

Following figure shows the six areas of cloud computing environment where instrument and software require attestation and that six areas are-

1. Security and data at rest.
2. Security and data in transits.

3. Authentication of users /applications/processes.
4. Robust separation of data belonging to different customs.
5. Cloud legal and regulatory issues.
6. Incident-response.

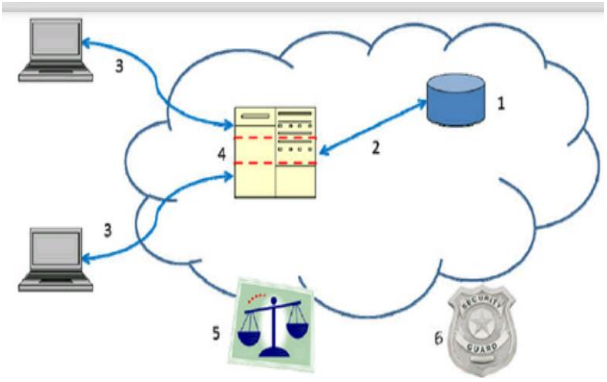

Fig- Areas for security concren in cloud computing.

Classification of Security Issues in Cloud Computing

The security issues in cloud computing can be categorized into the following three broad classes:

- Traditional security concerns
- Availability issues
- Third party data control-related issues

- **Traditional security concerns**

These security issues caries computer and network attacks that will be made possible or at least handily by moving to the cloud. Cloud supplier ripost to this concern by discussing that their security measure and possesses are more useful and proven than that of average company. Another discussion made by the Jenicho forum(Don't cloud vision) is: " it could be simple to protect the information if its administrator by a third party rather than the in-house, if companies are worried about interior threat, in more, it may be simple to enforce security through contract with online service supplier than through interior controls "

Concern in the traditional security includes following

1. VM-level attack

Insecurities have found in virtual pc's and virtual servers. Dealer such as third party brigade reduce potential VM-level insecurities through monitoring and firewall

2. Phising cloud provider

Phishers and other social engineers have new attack vector. Salseforce.com warns the customers about it

3. Expanded network attack surface

The cloud user must secured the platform and interact with the cloud. In many cases the task is problematic bye the cloud being outside the firewall

4. Authentication and Authorizations

The enterprise authentication and authorization formation does not surely extend in cloud

Availability issues

This concern focus on complicated application and data being available

Third party data control

The licit outcome of data and applications being picked by third party are very critical and not well understood. This is also potential shortage of control and transparency when third party picked the data.

Following are the concerns of third party data control

1. Due diligence
2. Auditability
3. Contractual obligation
4. Cloud provider espionage

The worry of theft of company's important information by cloud supplier.

III. APPLICATION SECURITY

Cloud environment-by virtue of their elasticity, clearness, and continually public availability challenge many basic assumption about applications security. Some of the assumptions are well understood, but many are not. This section is about how cloud computing impact security over the lifetime an application from design to operation to final touch. This guideline is for all stakeholders such as application designer, operational personnel, security professional, and technical management on how to reduced the risk and manage convection within the cloud computing applications.

Cloud computing is nothing but the challenge beyond the layers of Software as a Service, Infrastructure as a Service, Platform as a Service. Cloud dependent software applications needs a design rigor same as to application residing in classic DMZ.

Following are the major aspects of application security

1. Application security Architecture

Most of the applications are depends on the various systems in reality. With cloud computing, application faith can be highly dynamic. Cloud properties makes configuration management and outgoing provisionary expressively more critical than architecture modifications to assure application security.

2. Compliance

Compliance clearly influencing data, but it also affect applications and possesses

3. Software development lifecycle

Cloud computing influences all aspect of software development lifecycle spanning application architecture, deployment, maintenance, management and development.

IV. CONCLUSIONS

Cloud computing is very new concept that have number of benefits for its users; but it also having some security problem which may reduce its performance. Since cloud computing prestige many technologies, it also heirdom their security issues. Web application, data hosting and virtualization have been looked over traditionally, but some of the solution available are useless as they are immature or not exists. We have present some security issues for cloud: IaaS, SaaS,PaaS which changes depending on the situation. As describe in this paper storage, virtualization and network are the most biggest security problems in cloud computing.

.

ACKNOWLEDGMENT

We take this opportunity to thank our project guide for her valuable guidance and for providing all the necessary facilities and her suggestions

REFERENCES

[1] Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011.Online. Available: http://www.gartner.com/it/page.jsp?id=1454221 Accessed: 15-Jul-2011

[2] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: Statistic Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China Springer Berlin, Heidelberg, pp 347–358

[3] Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Futur Network(ICFN'10),Sanya,Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 9397

[4] Cloud Security Alliance (2011) Security guidance for critical areas of focus inCloud Computing V3.0 Available: https://cloudsecurityalliance.oguidance/csaguide.v3.0.pd

[5] Marinos A, Briscoe G (2009) Community Cloud Computing. In:1st International Conference on Cloud Computin (CloudCom), Beijing, China.Springer-Verlag Berlin, Heidelberg

[6] Centre for the Protection of National Infrastructure (2010) Informatio Security Briefing01/2010CloudComputing.Available:http://www.cpni.guk/Documents/Publications/2010/20-ISB_cloud_computing.pdf

[7] Khalid A (2010) Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10),

[8] Barham, P., Dragovic, B., Fraser, K., Hand, S.,Harris, T., Ho, A., Neugebauer, R., Pratt, I., and Warfield, A. (2003). Xen and the Art of Virtualization. Technical Report, University of Cambridge. Available online www.cl.cam.ac.uk/research/srg/netos/papers/2003- xensosp.pdf (Accessed on:Januar2013).

[9] Bhattacherjee, B., Abe, N., Goldman, K., Zadrozny,B., Chillakuru, V. R., Del Caprio, M., and Apte, C (2006). Using Secure Coprocessors for Privacy Preserving Collaborative Data Mining and Analysis.In 41 Proceedings of the 2nd

[10] International Workshop on Data Management on New Hardware (DaMoN'06), Chicago, Illinois, USA, June, 2006 Article No 1,New York: ACM Press.

