International Journal of Advanced Research in
Engineering and Applied Sciences
ISSN: 2278-6252

SECURITY ANALYSIS OF CLOUD COMPUTING

Anju Chhibber*

Dr. Sunil Batra**

Abstract: *Cloud computing is a model that uses the concept of utility computing that gives on-demand services to the end users. Cloud computing has the flexibility to produce shared resources over the internet and avoid serious installation price for it. However in conjunction with those benefits there's additionally a chance wherever a malicious user can infiltrate the cloud by impersonating a legitimate user that affects many shoppers who are sharing the cloud. This paper explore the cloud security problems faced by cloud service consumer such as data, privacy, and infected application and security problems and discuss some remedial measure to scale back the security risk.*

*Lecturer, Department of Computer Science & Applications, Guru Nanak Khalsa Inst. of Tech. & Management Studies (GNKITMS), Yamuna Nagar, India

**Assistant Professor, Department of Computer Applications, Chandigarh Group of Colleges Landran, Mohali (Pb), India

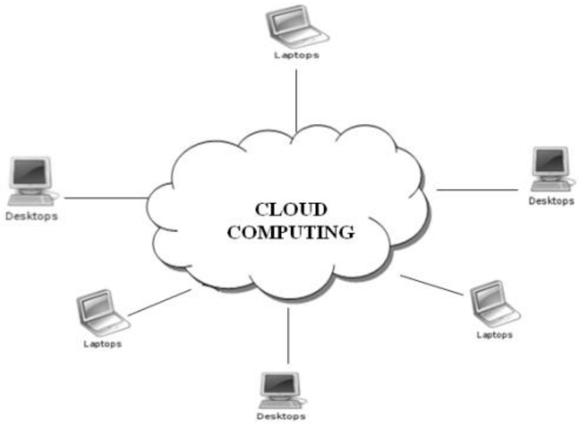
1. INTRODUCTION

'Cloud computing' is an emerging information technology for storing, processing and use of data from remotely located computers that can be accessed over the internet. This provides unlimited computing power on demand to users, which does not require major capital investments to fulfill their needs. In addition to that with the help of an internet connection they can retrieve their data from anywhere.

There are three types of cloud which includes private, public and hybrid cloud. The private cloud is owned by a single organization and public clouds are shared on a larger scale. Private cloud provides better control and more flexibility. Private Cloud and Public Cloud jointly makes Hybrid cloud, and this cloud is used by most of the industries. The advantages of cloud computing are very appealing but nothing is ideal. Cloud got several problems once it involves security particularly on data thievery, data loss and Privacy. This paper explores the cloud security threats and discusses some solutions to handle the security issue.

2. CLOUD COMPUTING SECURITY THREATS

The biggest challenge in implementing successful Cloud computing technologies is managing the security. As the sensitive applications and data are moved into the cloud data centers, run on virtual computing resources in the form of virtual machine which may cause many security concerns. Top seven security threats to cloud computing that are discovered by "Cloud Security Alliance" (CSA) are



a) Nefarious Use of Cloud Computing: It is the top threat identified by the CSA. In this approach attackers can penetrate a public cloud to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.

b) Insecure API (Application Programming Interfaces): APIs are set of software interfaces that are used by customers to interact with cloud services. When third parties begin to create that application then user take risks with the supply, confidentiality and integrity of data.

c) Shared Technology Vulnerabilities: As cloud provider platform being shared by different user there may be possibility that information belonging to different customers reside on same data center. Therefore Information leakage may arise as by mistake information for one customer is given to other.

d) Data Loss/Leakage: Data loss is a common problem in cloud computing. If the cloud computing service provider close up his services due some financial or legal problem then there will be a loss of data for the user.

e) Traffic Hijacking: Traffic hijacking is another issue that cloud users need to be aware of. These threats include man-in-the-middle attacks, spam campaigns and denial-of service attacks.

f) Malicious insiders: Such threats include fraud, damage and theft or loss of confidential information caused by trusted insiders. The malicious insiders can have the ability to infiltrate organizations and assets like productivity losses, brand damage and financial impact.

3. EXISTING SOLUTIONS FOR SECURITY THREATS

a) Mirage Image Management System: The integrity of VM images are the foundation for the overall security of the cloud. In this system use of Filters alleviate the risk in an efficient way. This system stores all the revisions which allow the user to go back to the previous version. The default access permission for an image is private so that only owner and system administrator can access the image and hence untrusted parties cannot access the image.

b) Client Based Privacy Manager: client based privacy manager helps to reduce the risk of data leakage and loss of privacy of the sensitive data processed in the cloud, and provides additional privacy related benefits.

c) Transparent Cloud Protection System (TCPS): It is a protection system which is intended to protect the integrity of guest Virtual Machines (VM) by allowing the host to monitor guest VMs and effective in detecting most kind of attacks. The system can detect an intrusion try over a guest and, if needed by the safety policy, takes applicable actions against the attempt or against the compromised guest.

4. OTHER EXISTING SOLUTIONS TO MANAGING CLOUD COMPUTING SECURITY

Managing and controlling Cloud issues will need to address but not limited to the following:

a) Cloud Governance: Cloud computing policies and procedures should be put in place to protect the cloud from potential of threats, hacks and the loss of information. The protection of data in the cloud is a key consumer concern particularly for committing fraudulent activities and financial exploitation. With governance and security in place, Cloud computing can be used safely and with confidence.

b) Cloud Transparency: Transparent security will make compulsory for cloud providers to disclose adequate information about their security policies and practices. SLA is one of the most significant protocols to ensure transparency within Cloud computing environment. The SLA is the only legal agreement between the service provider and client which includes the following rules:

i. Services to be delivered, performance,

ii. Tracking and Reporting

iii. Legal Compliance

iv. Security responsibility

c) Cloud Computing Security Impact: As computer makers, employers and universities install cloud based tools on desktops, several users could fail to understand that they're actually victimisation an online based service. A HTTPS encrypted connection takes significantly more processing power and memory for a Web server to provide than a normal web connection.

WS-Security assists with SOAP messages by shaping the header that carries the WS-Security extensions. The cloud computing moves a lot of of a user’s traditional activity to the online browser. internet browsers typically store all of a user’s saved passwords, browsing history and other sensitive data in a single place. as such it's doable for malicious websites to take advantage of browser to steal data related to different existing or previous browsing sessions, like a logged in email account or on-line banking session. it's for this reason that some security specialists suggest that customers use one web browser for general surfing, and another for additional sensitive tasks, like online banking. Potential Cloud organizations ought to remember that it's going to become easier for attackers to threaten clouds by moving towards one cloud interface.

5. CONCLUSION

Although Cloud computing can be seen as a new technology which revolutionize the way of using the Internet. However one must be very careful to understand the limitations and security risks posed in utilizing these technologies. In this paper key security challenges are highlighted which are currently faced by cloud industry.

BIBLIOGRAPHY

1. Dawei Sun, G. C. (2011). Surveying and Analyzing Security, Privacy and Trust Issues. *Advanced in Control Engineering and Information Science* , 2852 – 2856.
2. Dimitrios Zissis, D. L. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems , 28* (3), 583-592.
3. Kshetri, N. (4 July 2012). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy* , [In Press].
4. Latifa Ben Arfa Rabai, M. J. (2012). A cybersecurity model in cloud computing environments. *Journal of King Saud University – Computer and Information Sciences* (25), 63-75.
5. Ramgovind S, E. M. (n.d.). The Management of Security in Cloud Computing.
6. Shilpashree Srinivasamurthy, D. Q. (n.d.). Survey on Cloud Computing Security.
7. Winkler, V. (. (2011). *Introduction to Cloud Computing and Security.* Cloud Computer Security Techniques and Tactics.