Security Issues and Challenges in Cloud Computing

Arvind Jaiswal
Asst. Professor, FCA,
Acropolis Institute of Technology and Research, Indore (M.P.), India

Abstract - Cloud computing is a promising technology to facilitate the development of large-scale, on-demand, flexible computing infrastructures. Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. But without security embedded into innovative technology that supports cloud computing, businesses are setting themselves up for a fall. The trend of frequently adopting this technology by the organization automatically introduced new risk on top of existing risk. Obviously, putting everything into a single box i.e. into the cloud will only make it easier for hacker. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. This paper presents an overview and the study of the cloud computing along with several securities and challenging issues.

Keywords **- Cloud Computing, Virtualization, Security Issues, Threats.**

I. INTRODUCTION

The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service with all computing resources visualized as services and delivered over the Internet. Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture, Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while their software and data are stored on the servers. Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. In a cloud computing environment, the entire data reside over a set of networked resources, enabling the data

to be accessed through virtual machines. Since these data centers may lie in any corner of the world beyond the reach and control of users, there are multifarious security and privacy challenges that need to be understood and taken care of. This paper presents a categorization of security issues for Cloud Computing focused in the so-called SPI model (SaaS, PaaS and IaaS) and identifying the important threats found in the literature related to Cloud Computing and its environment.

II CLOUD COMPUTING

The National Institute of Standard and Technology defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as Amazon, Google, IBM etc. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users. Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for the person to store down on remote cloud servers. These gives the following three sensitive states that are of particular concern within the operational context of cloud computing:

- The transmission of personal sensitive data to the cloud server
- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one.

III RELATED WORKS

A. Cloud Information Security Objectives

The Data and Analysis Center for Software (DACS) requires that software must exhibit the following three properties to be considered secure:-

- **Dependability -** Software that executes predictably and operates correctly under a variety of conditions, including when under attack or running on a malicious host.
- **Trustworthiness** - Software that contains a minimum number of vulnerabilities or no vulnerabilities or weaknesses that could sabotage the software's dependability.
- **Survivability** - Software that is resistant to or tolerant of attacks and has the ability to recover as quickly as possible with as little harm as possible.

B. Security Issues in Cloud Computing

1. Software-as-a-service security issues - SaaS provides application services on demand such as email, conferencing software, ERP, CRM etc. SaaS users have less control over security among the three fundamental delivery models in the cloud. The adoption of SaaS applications may raise some security concerns which are as follows:

(a) Application security - These applications are typically delivered via the Internet through a Web browser. However, flaws in web applications may create vulnerabilities for the SaaS applications. Attackers have been using the web to compromise user's computers and perform malicious activities such as steal sensitive data.

(b) Data security - Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security. In SaaS, organizational data is often processed in plaintext and stored in the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and stored.

(c) Accessibility - Accessing applications over the internet via web browser makes access from any network device easier, including public computers and mobile devices. However, it also exposes the service to additional security risks.

2. Platform-as-a-service security issues - PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers. As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: security of the PaaS platform itself (i.e., runtime engine), and security of customer applications deployed on a PaaS platform. PaaS brings some data security issues that are described as follows:

(a) Third-party relationships - PaaS does not only provide traditional programming languages, but also does it offer third-party web services components such as mashups. Mashups combine more than one source element into a single integrated unit. Thus, PaaS models also inherit security issues related to mashups such as data and network security.

(**b) Development Life Cycle -** From the perspective of the application development, developers face the complexity of building secure applications that may be hosted in the cloud. The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security.

3. Infrastructure-as-a-service security issues - IaaS provides a pool of resources in the form of virtualized systems, which are accessed through the Internet. Users are entitled to run any software with full control and management on the resources allocated to

them. Here are some of the security issues associated to IaaS -

(a) Virtualization - Virtualization allows users to create, copy, share, migrate and roll back virtual machines, which may allow them to run a variety of applications. However, it also introduces new opportunities for attackers because of the extra layer that must be secured.

(b) Virtual machine monitor - The Virtual Machine Monitor or hypervisor is responsible for virtual machines isolation; therefore, if the VMM is compromised, its virtual machines may potentially be compromised as well. The VMM is low-level software that controls and monitors its virtual machines, so as any traditional software it entails security flaws.

(c) Shared resources - VMs located on the same server can share CPU, memory, I/O and others. Sharing resources between VMs may decrease the security of each VM. For example, a malicious VM can infer some information about other VMs through shared memory or other shared resources without need of compromising the hypervisor.

IV SECURITY CHALLENGES OF CLOUD COMPUTING

Cloud computing is an emerging technology with shared resources and lower cost that relies on pay per use according to the user demand. Due to its characteristics, it may face lots of threats and challenges in the scopes of security. In this section, these issues are explained and discussed-

(a) Data Loss/Leakage - Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe.

(b) Multi-location of the private data - It is rather dangerous, if the business stores its private data in the third party's device. In this sense, the businesses' private data are sitting in someone else's computer. It is rather important for a company to understand in which country its data will be hosted.

(c) Reused IP Addresses - When a particular user moves out of a network, then the IP-address associated with him (earlier) is assigned to a new user. Sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the earlier user.

(d) Denial of Service Attacks - A DoS attack is an attempt to make the services assigned to the authorized users unavailable. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user.

V SOLUTIONS FOR SECURITY ISSUES IN CLOUD COMPUTING

Investigation Support: Audit tools provided to the users to determine how their data is stored, protected, used and verify policy enforcement. But investigation of illegal activity is quite difficult because data for multiple customers may be collocated and may also be geographically spread across set of hosts and datacenters. To solve this audit tools must be contractually committed along with the evidence.

Network Security: A user can deny the access of any Internet based service by using IP Spoofing which can be a cause of security harm. To solve this we can use Digital Signature technique. SSL (Secure Socket Layer) Protocol is used for managing security of message transmission on The Internet which also avoid resource hacking.

Encryption Algorithm: Obviously cloud service providers encrypt the user's information using strong encryption algorithm. But problem is that encryption accident can make data totally unusable and encryption also complicates the availability. To solve this problem the cloud provider must provide evidence that encryption scheme were designed and tested by experienced specialists.

Backup: Natural disaster may damage the physical devices that may cause data loss. To avoid this problem backup of information is the key of

assurance of service provided by vendor. V SOLUTIONS FOR SECURITY ISSUES IN CLOUD COMPUTING

Investigation Support: Audit tools provided to the users to determine how their data is stored, protected, used and verify policy enforcement. But investigation of illegal activity is quite difficult because data for multiple customers may be collocated and may also be geographically spread across set of hosts and datacenters. To solve this audit tools must be contractually committed along with the evidence.

Network Security: A user can deny the access of any Internet based service by using IP Spoofing which can be a cause of security harm. To solve this we can use Digital Signature technique. SSL (Secure Socket Layer) Protocol is used for managing security of message transmission on The Internet which also avoid resource hacking.

Encryption Algorithm: Obviously cloud service providers encrypt the user's information using strong encryption algorithm. But problem is that encryption accident can make data totally unusable and encryption also complicates the availability. To solve this problem the cloud provider must provide evidence that encryption scheme were designed and tested by experienced specialists.

Backup: Natural disaster may damage the physical devices that may cause data loss. To avoid this problem backup of information is the key of assurance of service provided by vendor.

VI. CONCLUSION AND FUTURE WORK

Cloud Computing, envisioned as the next generation architecture of IT Enterprise is a talk of the town these days. Although it has revolutionized the computing world, it is prone to manifold security threats varying from network level threats to application level threats. In order to keep the Cloud secure, these security threats need to be controlled. Auditing of the cloud at regular intervals needs to be done to safeguard the cloud against external threats. In this paper, various security concerns for Cloud computing environment from multiple perspective and the solutions to prevent them have been presented. In future, concrete standards for cloud computing security can be developed. To provide a secure data access in cloud, advanced encryption techniques can be used for storing and retrieving data from cloud. Also proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data.

REFERENCES

[1] Barrie Sosinsky - Cloud Computing Bible: Wiley Publishing, Inc.

[2] Ronald L.Krutz and Russell Dean Vines - Cloud Security: A Comprehensive Guide to Secure Cloud Computing.

[3] Christian Baun, Marcel Kunze, Jens Nimis and Stefan Tai - Cloud Computing: Web-based Dynamic IT Services.

[4] Rajkumar Buyya, James Broberg, Andrzej Goscinski - Cloud Computing: Principles and Paradigms.

[5] A.Agarwal - The Security Risks Associated with Cloud Computing - International Journal of Computer Applications in Engineering Sciences, 2012.

[6] Mahbub Ahmed, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation" - IEEE International Conference on Embedded and Ubiquitous Computing, 2013.

[7] Michael glas and paul Andres, "An Oracle white paper in enterprise architectureachieving the cloud computing vision", CA-U.S.A, Oct 2010.

[8] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), 39-51, University of Texas, USA, April-June 2010.

[9] Joachim Schaper, 2010, "Cloud Services", 4th IEEE International Conference on DEST,Germany.

[10] Dr. Gurdev Singh, Shanu Sood, Amit Sharma, "CM- Measurement Facets for Cloud Performance", IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[11]. R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing," The World Privacy Forum, 2009. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[12] Dukaric, R. and Juric, M.B. (2013). Towards a unified taxonomy and architecture of cloud frameworks. Future Generation Computer Systems, 29, 1196–1210. doi:10.1016/j.future.2012.09.006

[13] Emam, A.H.M. (2013). Additional Authentication and Authorization using Registered Email-ID for Cloud Computing. International Journal of Soft Computing and Engineering, 3(2), 110-113.