Volume 6, Issue 4, April 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Study of Threats Related With Cloud Computing

Akshika Aneja

Assistant professor, Department of Computer Science,
GNDU, Amritsar, Punjab, India

Abstract— Cloud computing security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Malicious activities from illegal users have threatened this technology with issues such as data misuse, inflexible access control and limited monitoring. The occurrence of these threats may result into damaging or illegal access of critical and confidential data of users. This research paper describes the characteristics (threats, vulnerabilities) associated with a cloud and some measures for enhancing cloud security.

Keywords— Illegal access, Threats, Vulnerabilities, data loss.

I. INTRODUCTION

The traditional era of computing involves the use of software, hardware and storage to achieve the required computational service whereas cloud computing has isolated the services from resources (networks, storage, servers). The required services are provided to the users by utilizing the resources of provider. Users are no longer required to purchase hardware, software or to manage storages. Due to the evolution of this technology users are required to pay for cloud services on consumption basis. New cloud based business models are being discussed, defined, and implemented as solutions in form of on-demand services that allows businesses to enhance their efficiency and scalability. Success or failure of this technology relies on users' trust whether the service provided is reliable, available and secure. Before starting the journey to cloud, organizations must considers the possible threats and vulnerabilities that may convert their dreams of enhancing scalability and saving management cost into a nightmare of data loss and misuse.

II. CLOUD COMPUTING THREATS

As we already mentioned, there are several significant threats that should be considered before adopting the paradigm of cloud computing, these threats are described as follows:

A. Immoral Use of Cloud

Cloud providers facilitate the users with various types of services including unlimited bandwidth and storage capacity. Some cloud service providers offer free limited trial periods that gives an opportunity for hackers to access the cloud immorally, their impact includes decoding and cracking of passwords, launching potential attack points and executing malicious commands. Spammers, malicious code authors and other cybercriminals can conduct their activities with relative impunity, as cloud service providers are targeted for their weak registration systems and limited fraud detection capabilities. For example some cybercriminals use rich content applications such as flash files that enable them to hide their malicious code and utilize users' browsers to install malware.

B. Insecure Interfaces and APIs

Cloud users are using software interfaces and APIs to access and manage the cloud services. These APIs need to be secured because they play an integral part during provisioning, management, orchestration and monitoring of the processes running in a cloud environment. The security and availability of cloud services is dependent upon the security of these APIs so they should include features of authentication, access control, encryption and activity monitoring. APIs must be designed to protect against both accidental and malicious attempts to avoid threats. If cloud service provider relies on weak set of APIs, variety of security issues will be raised related to confidentiality, integrity, availability and accountability such as malicious or unidentified access, API dependencies, limited monitoring/logging capabilities, inflexible access controls, anonymous access, reusable tokens/paswords and improper authorizations.

C. Insider attacks

Insider attacks can be performed by malicious employees at the provider's or user's site. Malicious insider can steal the confidential data of cloud users. This threat can break the trust of cloud users on provider. A malicious insider can easily obtain passwords, cryptographic keys and files. These attacks may involve various types of fraud, damage or theft of information and misuse of IT resources. The threat of malicious attacks has increased due to lack of transparency in cloud provider's processes and procedures . It means that a provider may not reveal how employees are granted access and how this access is monitored or how reports as well as policy compliances are analyzed. Additionally, users have little visibility about the hiring practices of their provider that could open the door for an adversary, hackers or other cloud intruders to steal confidential information or to take control over the cloud. The level of access granted could enable attackers to collect confidential data or to gain complete control over the cloud services with little or no risk of detection. Malicious insider attacks can damage the financial value as well as brand reputation of an organization.

D. VM Technology

Due to the cloud virtualization, cloud providers are residing the user's applications on virtual machines (VMs) within a shared infrastructure. The VMs are virtualized based on the physical hardware of cloud provider. In order to maintain the security of users, providers are isolating the VMs from each other so if any of them is malicious, it will not affect the other VMs under the same provider. The VMs are managed by hypervisor in order to provide virtual memory as well as CPU scheduling policies to VMs. As the hypervisor is main source of managing a virtualized cloud platform, hackers are targeting it to access the VMs and the physical hardware, because hypervisor resides between VMs and hardware, so attack on hypervisor can damage the VMs and hardware. Strong isolation should be employed to ensure that VMs are not able to impact or access the operations of other users running under the same cloud service provider. Several vendors such as Xen and KVM are providing strong security mechanisms of securing the cloud hypervisors, but still it is identified that sometimes security of VMs is compromised.

E. Loss of data

Data loss can occur due to operational failures, unreliable data storage and inconsistent use of encryption keys. Operational failure refers to deletion or alteration of records without a backup of the original content that can take place intentionally or unintentionally. Unreliable data storage refers to saving of data on unreliable media that will be unrecoverable if data is lost. The inconsistent use of encryption keys will result into loss and unauthorized accesses of data by illegal users that will lead to the destruction of sensitive and confidential information. Example of data loss is Twitter hacks. The online accounts of Twitter accessed by hackers and their numerous sensitive corporate documents were stolen. These documents were housed in Google's online web office service Google Docs. Although Google was not the one to be blamed for security break-in as the security of documents from twitter was not efficient enough. Instead, the entire company data was only one password crack away from discovery. It's clear from this example that data loss or leakage can damage one's brand, reputation and cause a loss that may significantly impact employee, partner and users' morale as well as trust. Loss of core intellectual property can have competitive and financial implications beside the compliance violations and legal consequences.

F. Hijacking

Account or service hijacking refers to unauthorized access gained by attackers to control the users' accounts, such as phishing, fraud and exploitation of software vulnerabilities. For example if an attacker gains access to users' credentials, they can spy on their activities/transactions, manipulate their data, return falsified information and redirect them to illegitimate sites. Users' account or service instances may become a new base for the attackers who can leverage the cloud service providers' reputation by launching subsequent attacks. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Authentication and authorization through the use of roles and password protecting is a common way to maintain access control when using web-browsers to access cloud computing systems. However, this method is not sufficient enough to secure sensitive and critical data.

G. Unknown Risk Profile

It is important for the users to know software versions, security practices, code updates and intrusion attempts. While adopting cloud computing services, these features and functionality may be well advertised but what about the details or compliance of the internal security procedures, configuration hardening, patching, auditing and logging. Users must be clarified how and where their data and related logs are stored. However, there is no clear answer that leaves users with an unknown risk profile that may include serious threats.

III. MEASURES FOR ENHANCING CLOUD SECURITY

With employees, customers, business partners, suppliers and contractors increasingly accessing corporate applications and data with mobile devices from the cloud, protecting the edge of the network is no longer enough. Some important measures to help ensure security in the cloud are as follows:

1. Attention on previlaged users

People within your organisation who are privileged users, – such as database administrators and employees with access to highly valuable intellectual property – should receive a higher level of scrutiny, receive training on securely handling data, and stronger access control.

2. Limit data access based on user context

Change the level of access to data in the cloud depending on where the user is and what device they are using. For example, a doctor at the hospital during regular working hours may have full access to patient records. When she's using her mobile phone from the neighborhood coffee shop, she has to go through additional sign-on steps and has more limited access to the data.

3. Identify sensitive or valuable data

Identify databases with highly sensitive or valuable data and provide extra protection, encryption and monitoring around them.

4. Extend security to the device

Ensure that corporate data is isolated from personal data on the mobile device. Install a patch management agent on the device so that it is always running the latest level of software. Scan mobile applications to check for vulnerabilities.

5. Use network protection devices

The network still needs to be protected – never more so than in the cloud. Network protection devices need to have the ability to provide extra control with analytics and insight into which users are accessing what content and applications.

6. Audit trail

Security devices, such as those validating user IDs and passwords, capture security data to create the audit trail needed for regulatory compliance and forensic investigation. The trick is to find meaningful signals about a potential attack or security risk in the sea of data points. Adding a layer of advanced analytics – a security intelligence layer – brings all of this security data together to provide real-time visibility into the both the data centre and the cloud infrastructure.

IV. CONCLUSION

When your business grows, your IT needs grow too. The scalability and speed of deployment offered by cloud computing means you can expand your IT provision instantly to meet increased requirements, and you can also scale it down again whenever you want. Moving to a cloud computing model can help your organization to survive in a tough economic climate, equipping you with the latest business tools and giving you access to advanced technologies at a fraction of the cost of purchasing and running the same systems in-house.

In this research paper, the characteristics of a stormy cloud that contains threats and vulnerabilities have been discussed. Cloud computing has a dynamic nature that is flexible, scalable and multi-shared with high capacity that gives an innovative shape of carrying out business . However,beside these benefits there are deadly threats encountered in this technology. Therefore, there is still tremendous opportunity for researchers to make revolutionary contributions in this field and bring significant impact of their development to the industry. There is need to develop and design in-depth security techniques and policies in terms of people, processes and technology.

REFERENCES

[1] E., Mathisen, ―Security challenges and solutions in cloud computing,‖ in Digital Ecosystems and Technologies Conference (DEST), Proceedings of the 5th IEEE International Conference on, 2011, pp. 208-212

[2] S. Farrell, ―Portable Storage and Data Loss,‖ Internet Computing, IEEE, vol. 12, no. 3, pp. 90-93, 2008.

[3] Karthick Ramachandran, Thomas Margoni and Mark Perry, ―Clarifying Privacy in the Clouds‖ in CYBERLAWS 2011:The Second International Conference on Technical and Legal Aspects of the e-Society, IARIA,2011.

[4] S., Subashini, V. Kavitha. ―A survey on security issues in service delivery models of cloud computing‖. Journal of Network and Computer Applications, vol.34, pp.1-11, 2011.

[5] B. Grobauer, T. Walloschek, and E. Stocker, ―Understanding Cloud Computing Vulnerabilities,‖ Security & Privacy, IEEE, vol. 9, no. 2, pp.50-57, 2011.