Securing your Cloud Environment

Fatahiyya Ali Lawal
Department of Computer Science
SRM University Kattankulathur Chennai India

***Abstract*-Alongside its growth, cloud computing has seen an increase in criminal activities in the cloud. Cloud computing faces many threats as the physical workplace. Attackers use tactics such like social engineering or working from the inside. They take advantage of employees' use of social media and downloading of applications on company computers to send attacks over the web. They continue to take advantage of email with increasingly sophisticated viruses that bypass anti-virus tools. Hackers focus on targeting specific organizations with valuable data – attacking in a planned and professional way. All of these threats affect the cloud, the data center, and personal devices. This paper presents a review on the cloud computing security concepts as inherent within the context of cloud computing and cloud infrastructure.**

***Keywords: Cloud computing and Architecture, service models and Deployment, cloud security and Types*.**

I. INTRODUCTION

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications.Cloud computing is comparable to grid computing , a type of computing where unused processing cycles of all computers in a network are harness to solve problem too intensive for any standalone machine.

Fig1.1 Cloud Computing Architecture

Cloud computing allows the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

II. CHARACTERISTICS

The characteristics of cloud computing include on-demand self service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self service means that customers (usually organizations) can request and manage their own computing resources. Broad network access allows services to be offered over the Internet or private networks. Pooled resources means that customers draw from a pool of computing resources, usually in remote data centres. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

III. SERVICE MODELS

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In a Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications.

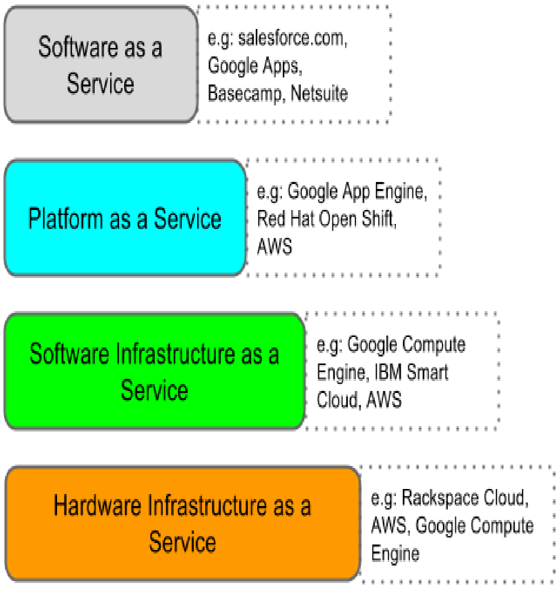
Software as a Service
e.g: salesforce.com, Google Apps, Basecamp, Netsuite
Platform as a Service
e.g: Google App Engine, Red Hat Open Shift, AWS
Software Infrastructure as a Service
e.g: Google Compute Engine, IBM Smart Cloud, AWS
Hardware Infrastructure as a Service
e.g: Rackspace Cloud, AWS, Google Compute Engine

Fig2.1 Cloud Computing service Models architecture.

A. DEPLOYMENT OF CLOUD SERVICES

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud. Generally speaking, services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud. In a private cloud, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party. In a community cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

A hybrid cloud is a combination of different methods of resource pooling (for example, combining public and community clouds).

B. WHY CLOUD SERVICES ARE POPULAR

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software licences, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations. In addition, cloud providers that have specialized in a particular area (such as e-mail) can bring advanced services that a single company might not be able to afford or develop. Some other benefits to users include scalability, reliability, and efficiency. Scalability means that cloud computing offers unlimited processing and storage capacity. The cloud is reliable in that it enables access to applications and documents anywhere in the world via the Internet. Cloud computing is often considered efficient because it allows organizations to free up resources to focus on innovation and product development.

Another potential benefit is that personal information may be better protected in the cloud. Specifically, cloud computing may improve efforts to build privacy protection into technology from the start and the use of better security mechanisms. Cloud computing will enable more flexible IT acquisition and improvements, which may permit adjustments to procedures based on the sensitivity of the data. Widespread use of the cloud may also encourage open standards for cloud computing that will establish baseline data security features common across different services and providers. Cloud computing may also allow for better audit trails. In addition, information in the cloud is not as easily lost (when compared to the (when compared to the paper documents or hard drives).

C. CLOUD SECURITY

To advance cloud computing, the community must take proactive measures to ensure security. Cloud computing presents an extension of problems heretofore experienced with the Internet. As mentioned, legal decisions will ultimately determine who “owns” the responsibility for securing information shared within clouds. To ensure that such decisions are informed and appropriate for the cloud computing environment, the industry itself should establish coherent and effective policy and governance to identify and implement proper security methods.

Fig 1.3 Cloud security

D. IMPORTANCE OF CLOUD SECURITY

As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker. Security and privacy both are concerns in cloud computing due to the nature of such computing approach (Bisong & Rahman, 2011). The approach by which cloud computing is done has made it prone to both information security and network security issues (Rakhmi, Sahoo & Mehfuz, 2013; Qaisar & Khawaja, 2012). Third party relationship might emerge as a risk for cloud environment along with other security threats inherent in infrastructural and virtual machine aspects (Hashizume et al., 2013). Factors like software bugs, social engineering, human errors make the security for cloud a dynamically challenging one (Kim, 2009). Intrusion detection is the most important role in seamless network monitoring to reduce security risks. If the contemporary IDSs (Intrusion detection Systems) are inefficient, the resultant consequence might be undetected security breach for cloud environment (Westphall et al., 2011).

E. TYPES OF CLOUD SECURITY

Modern Technology offered by cloud concept is facilitating the business world in an agile manner to increase the productivity. To augment cloud technology’s acceptance and implementation several security concerns need additional study in order to handle these issues appropriately.

Seven categories could be presented for future studies to concentrates on cloud’s security issues. Each of them are discussed under the points below.

a. Network Security

This category includes the problems related to network communications and configuration of cloud infrastructure. To overcome the problems related to network security issues in cloud services, similar privacy procedures and provisions should be adopted that are implemented on an existing local internal network .This way allows local network to be extended and implemented on a remote process.

Transfer Security:VPN(Virtual Private Network) mechanisms are required to protect distributed architecture of cloud from possible threats such as sniffing,spoofing,man-in-the-middle and side channel attacks. Possibility of threat increasing a distributed architecture as enormous resource is shared and large number of virtual machines are synchronized to involve a large amount of data to transfer in cloud.

Firewalling: Service providers cloud infrastructure is protected against both inside and outside threats by creating a firewall. What exactly firewall does is.

- It isolate the virtual machines
- Brilliantly filters address and ports
- Prevents denial of service(DOS)
- Detect external security assessment measures

Security configuration: protocol, systems and technologies used should be well configured to offer the mandatory level of security and privacy.

b. Interfaces

To use the cloud services one needs to have cloud interface. This interface is responsible for every issue that is related to user, administrative and programming interfaces.

- API: Programming interfaces (essential to Iaas and PaaS) must be sheltered from malwares in order to access virtualised resources efficiently.
- Administrative Interface: it remotely controls the resources in an IaaS model(Virtual Machine Management),controls the coding, deploying and testing in developing PaaS.it also controls user access and configuration of application tools for SaaS.
- User Interface: To ensure the security of the environment, it acts as the end user interface.
- Authentication: To access the cloud services certain authentication mechanisms are required. These authentication mechanisms are required to ensure the security measures, as the virtual environment is vulnerable to several attacks.

c. Data Security

For security issues protection of data is the basic thing. Data should be confidential. It is available to only authorised users.

- **Cryptography:** Encryption of data is most popular way to make it secure and sensitive. Almost every organisation, irrelevant to its industry and state is using this method to ensure the security of the data.
- **Redundancy:** This feature avoids the problem related to loss of data. Since, most of the business organisations are using IT services and they are totally relying on them. In this case availability and integrity of data must be guaranteed.
- **Disposal:** Disposal of basic data is commonly referred as deletion. Complete damage of data including logging references and secret backup registries is a prerequisite in cloud technology.

d. Virtualisation

This category includes the issues related to the used virtual technology in developing cloud environment. Virtualisation mostly have issues related to the management of virtual machines and is commonly known as hypervisor vulnerabilities.

- **Isolation:** Since, every resource either hardware or software in cloud environment is shared in between the virtual machines, so this might create an issue related to data leakage and cross-VM attacks by some of the malicious entities. Though, each machine is conceptually isolated with the other one but, still there are security threats, as every resource is shared including the memory and computational resources.
- **Hypervisor vulnerabilities:** The main component of virtualisation is hypervisor that is also referred as virtual machine management (VMM). Hypervisors security vulnerabilities are commonly the known one and it is easy to recognise them but still the solution to these vulnerabilities are limited. Complexities in getting the solution to hypervisor vulnerabilities demand more studies.
- **Data leakage:** If there is any shortage in virtual infrastructures' isolation controls then it can cause data leakage and reveal sensitive data of the user that can affect the confidentiality and integrity.
- **VM identification:** To ensure the security issues it is necessary for controls to identify every virtual machine that is being used for a particular process or saving files.
- **Cross-VM attacks:** Any virtual machine is exposed to another's attack and it happens whenever the cryptographic keys of a machine are stolen by another one. This is known as cross-VM attack.

e. Governance

In cloud computing issues associated to lose the controls from administration and security are classified under governance.

- **Data control:** Owner loses the control from data redundancy, location of the data, file systems and other related configurations whenever data moves to cloud.

- **Security control:** If there is any unsatisfactory Service Level Agreement (SLA) is in between service provider and the user/client then the provider could lose the governance from security mechanisms and policies. Losing the controls over the governance can restrict client-side susceptibility evaluation and breach tests.
- **Lock-in:** Due to the shortage of well-established standards (i.e. standards related to protocols and data formats) users generally depend upon the services of a particular service provider. And finally this results in user's inability in migrations and service termination.

f. Compliance

Compliance is related to service accessibility and assessment capability requirements. It includes certain points mentioned below.

- **Service Level Agreements (SLA):** Certain mechanisms which ensure the basic security measures need to be adopted. Availability of services is also mentioned in SLAs.
- **Loss of service:** Since, there is a strong interconnection in between different services in cloud environment (e.g. SaaS and IaaS have interconnections as a SaaS is provided by an IaaS with the help of a virtualised infrastructure), so interruption in services is also possible. Due to this reason, user-side data redundancy and certain disaster recovery strategies are recommended if it is relevant.
- **Audit:** Customers, providers and third-party members are allowed to perform security and availability assessments with the help of certain transparent and efficient methodologies. A transparent API is being developed to get the solution for this problem that will perform automated auditing and other necessary roles.
- **Service conformity:** Depending upon the SLAs predefined and basic customer needs contractual responsibility and complete service requirements should be confirmed.

g. Legal Issues

This issue is related to facets regarding judicial requirements and law (e.g. availability of data at multiple locations and privilege management).

- **Data location:** By subpoena law-enforcement procedures customers' data depending upon different geographic locations are held in multiple jurisdictions and are affected directly or indirectly.
- **E-discovery:** According to the law-enforcement procedures, for an investigation regarding a particular user, a common hardware for more than one user could be removed. This results in data revelation.
- **Provider privilege:** Provider insiders' malicious activities could be possible threats to user data's confidentiality, availability and integrity.
- **Legislation:** It is related to the judicial concerns to new concepts of cloud computing.

IV. CONCLUSION

Cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. Cloud computing is a great opportunity and lucrative option both to the businesses and the attackers – either parties can have their own advantages from cloud computing. The vast possibilities of cloud computing cannot be ignored solely for the security issues reason – the ongoing investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of motivation. The security issues could severely affect cloud infrastructures. Security itself is conceptualized in cloud computing infrastructure as a distinct layer (Dukaric & Juric, 2013). Security for cloud computing environment is a non-compromising requirement. Cloud computing is inevitable to become the ideal (and possibly the ultimate) approach to business computing though the security barriers along with other issues need to be resolved for cloud computing to make it more viable (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011) . Yet, given its total advantages and dynamism and provided it is deployed within an integrated and secured infrastructural framework, cloud computing can offer virtual ownership and access to 'super computers' without procuring them physically.

REFERENCES

[1]. Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103

[2]. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011).Cloud computing — The business perspective. Decision Support Systems, 51, 176–189. doi:10.1016/j.dss.2010.12.006

[3]. 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

[4]. Kim, W. (2009). Cloud Computing: Today and Tomorrow. Journal of Object technology, 8(1), 65-72.

[5]. King, N.J. and Raja, V.T. (2012).Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Reviews, 28, 308-319.

[9]. Rashmi, Sahoo, G. and Mehfuz, S. (2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. International Journal on Cloud Computing: Services and Architecture, 3(4), 1-11. Doi: 10.5121/ijccsa.2013.3401

[10]. Westphall, C.B., Westphall, C.M., Koch, F.L., Rolim, C.O., Vieira, K.M., Schulter, A., Chaves, S.A., Werner, J., Mendes, R.S., Brinhosa, R.B., Geronimo, G.A. and Freitas, R.R. (2011). Management and Security for Grid, Cloud and Cognitive Networks. Revista de Sistemas de Informação da FSMA, 8, 8-

[11]. Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security Technical Report, 16,102-107.

[6]. Youssef, A.E. (2012). Exploring Cloud Computing Services and Applications. Journal of Emerging Trends in Computing and Information Sciences, 3(6),838-847 doi:10.1016/j.istr.2011.08.005

[7]. Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security

[8] Agarwal, A. and Agarwal, A. (2011). The Security Risks [21].Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.

[12]. Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103

[13]. B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[14]. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, “On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[15]. Pring et al., “Forecast: Sizing the cloud; understanding the opportunities in cloud services,” Gartner Inc., Tech. Rep. G00166525, March 2009.

[16]. Aman Bakshi, Yogesh B. Dujodwala, “Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine,” ICCSN ’10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[17]. B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[18]. K. Hwang, S Kulkarni and Y. Hu, “Cloud security with virtualized defence and Reputation-based Trust management,” Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695- 3929 -4.