ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 2, pp: (108-113), Month: April - June 2019, Available at: www.researchpublish.com

A REVIEW ON CLOUD COMPUTING AND NETWORK SECURITY

[1]Mohd. Roshan Zameer, [2]Anil Kumar Pandey, [3]Kusum Kusum Sharma

M.Tech. Scholar, Assistant Professor, Assistant Professor, Department of Computer Science & Engineering, RSR RCET, Bhilai, Chhattisgarh, India

Abstract: **Cloud computing is an emerging technology that provides a flexible and scalable IT infrastructure to ensure business agility. There are different vulnerabilities and various threats to cloud computing. We have reviewed several cases where 'social sites application is infiltrated by attacks'. We have seen so many malware and scam attacks on social networks are seem to be common these days. Many such incident have come to the forefront in the last few years and the problem seem rising everyday. This proves that how malware writer focus on web as there primary target, and it has shown the vulnerability of social networking sites as well. In this paper several types of attacks are discussed, real world cases studied. And the solutions that providers developed are presented.**

Keywords: **Cloud Computing, Types of Cloud Computing, Cloud Storage, Network Security, Malware Injection.**

1. INTRODUCTION

Cloud computing has become the newest rave in the computing industry. Its ability to save business cost by eliminating the need to purchase huge amounts of software or software license for every employee, reducing the need of advanced hardware, eliminating the need for companies to rent physical space to store servers and databases, and shifting the workload from local computers that has appealed to cloud computing providers such as Amazon, Google, IBM, Yahoo, Microsoft, etc. In the past decades, the world of computation experienced some dramatic changes stand alone application to client-server architecture and from distributed to service oriented architecture. All the cloud computing providers are rushing to provide solutions in many ways from different perspectives, there are dozens of definitions of cloud computing. But only certain things are common

- On-demand self-service
- Ubiquitous network access
- Location independent resource pooling.
- Rapid elasticity
- Measured service

A. Types of Cloud Computing Services

1. Infrastructure as a Service (IaaS)

IaaS is the lowest level of cloud solutions and refers to cloud based computing infrastructure as a fully-outsourced service. An IaaS provider will delivered pre-installed and configured hardware or software through a virtualized interface. What the customers to do with the cloud services are up to them.

Benefits of IaaS Solutions

- Reduce total cost of ownership and capital expenditures
- Users pay for the service that they want on the go
- Access to enterprise-grade-IT resources and infrastructure

2. Platform as a Service (PaaS)

This type of cloud computing is similar to IaaS but is more advanced. With PaaS, apart from simply providing infrastructure, providers also offer a computing platform and solution stack as a service. The IT infrastructure may come with a graphic user interface, run-time system libraries, programming languages or an operating system.

PaaS services are mostly used by companies that need to develop, test, collaborate and deploy cloud solutions for particular applications. However hosting of application is done by the third party.

PaaS providers offer a fully configured sandbox and deployment environment for customers to develop, test and deploy their cloud applications.

Benefits of PaaS Solutions

- Community
- No more upgrades
- Lower cost
- Simplified Deployment

3. Software as a Service (SaaS)

Most people think of Software as a Service (SaaS) when talked about cloud services. SaaS providers provide fully functionally web-based applications on demand to customers. The applications are mainly targeted at business users and can include web conferencing , ERP, CRM, email, time management, project tracking among others.

Benefits of SaaS Solutions

- Raid Scalability
- Accessibility from any location
- Eliminates infrastructure concerns
- Bundled maintenance and support

4. Recovery as a Services (RaaS)

According to a Gartner report, 30 percent of midsize companies have adopted cloud recovery service. Recovery as a service (RaaS) solutions helps companies to replace their backup, archiving, disaster recovery and business continuity solutions in a single, integrated platform. RaaS providers protect and help the companies to recover entire data centers, servers (OS applications, configuration and data)

RaaS helps business to reduce the impact of downtime when disasters happen. RaaS is also referred as DRaaS (Disaster Recovery as a Service)

Benefits of RaaS Solutions

- Prevent temporary and permanent loss of critical company data
- Is a cost-effective way of recovering data
- Enables faster recovery while maintaining accuracy

B. Types Of Cloud Storage

1. Public Cloud Storage

Public cloud storage is where the enterprise and storage service providers are separate and there aren’t any cloud resources stored in the enterprises data center. The cloud storage provider fully manages the enterprises public cloud storage.

2. Personal Cloud Storage

Also known as mobile cloud storage, personal cloud storage is a subset of public cloud storage that applied to storing and individuals data in the cloud and providing the individual with access to data from anywhere. It also provides data syncing and sharing capabilities across multiple device. Apple icloud is an example of personal cloud storage.

3. Private Cloud Storage

A form of cloud storage where the enterprise and cloud storage provider are integrated in enterprises data center. In private cloud storage., the storage provider has infrastructure in the enterprises data center that is typically managed by the storage provider. Private cloud storage help resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

4. Hybrid Cloud Storage

It is a combination of public and private cloud storage where some critical data resides in the enterprises private cloud while other data is stored and accessible from a public cloud storage provider.

2. NETWORK SECURITY

Multiple real world cases where cloud computing were compromised and the ways the company mitigated the incident will be discussed. For each case the attack style will be briefly described, the details of the case will be presented and the prevention method will be discussed.

A. Different network security issues:

1. Data Breaches

A data breach in cloud is an incident that involves the unauthorized and illegal viewing, accessing or retrieval of data by an individual application or service. Data breach may involve personal information like health information, identifiable information or intellectual property.

2. XML Signature wrapping attack

Web servers offer designers enormous flexibility when it comes to employing integrity features. Usually in order to guarantee a message certain pre-defined parts of a SOAP message get signed.

Let us assume that a web service client sends a signed message to receiving web service. Ideally any malicious modification of signed data is detected by the web service unless the attacker is able to break the signature algorithm itself. However when executing a XML signature wrapping attack an attacker is able to change the content of the signed part without invalidating the signature. This attack is also known as XML Rewriting attack.

3. Hijack Of Account

In cloud account hijacking, a hacker uses a compromised email account to impersonate the account owner. Typically, account hijacking is carried out through phishing, sending spoofed email to the user, password guessing or a number of other hacking tactics. It is a type of identity theft in which the hacker uses a stolen account information to carry out malicious or unauthorized activity.

4. Malware Injection

In cloud Malware injection attack, an attacker tries to inject malicious service or virtual machine into the cloud.in this type of attack attacker creates it's own malicious service implementation module. The attack can appear in the form of code, scripts, active content and/or other software. When an instance of legitimate user is ready to run in the cloud server, there respective service accept the instance for computation in the cloud. The checking is done to determine the instance matches a legitimate existing service.

5. Insecure API's

Application programming Interfaces (APIs) gives user the opportunity to customize their cloud experience. However, APIs can be a threat to cloud security because of their very nature. Provisioning, management, orchestration and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. As the infrastructure of APIs grows to provide better service, the security risk increases along with it. The vulnerability of API lies in the communication that takes place between applications.

3. MALWARE INJECTION

In cloud Malware injection attack, an attacker tries to inject malicious service or virtual machine into the cloud.in this type of attack attacker creates it's own malicious service implementation module. The attack can appear in the form of code, scripts, active content and/or other software. When an instance of legitimate user is ready to run in the cloud server, there respective service accept the instance for computation in the cloud. The checking is done to determine the instance matches a legitimate existing service.

A. Types of Malware Injection Attack

1. SQL Injection attack

SQL injection attack targets the database underlying an application through a user input field. A destructive SQL command is given as a part of the input field which when substituted into the SQL query makes it a valid one but performs a unexpected harmful action

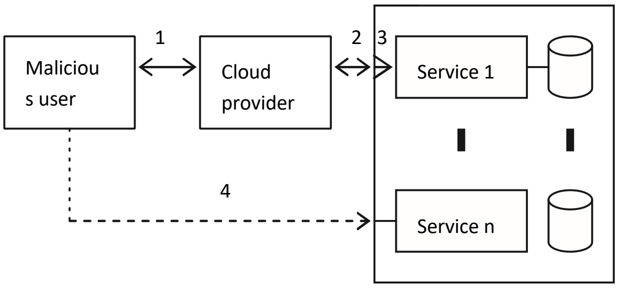

Fig. 3.A.1 Sql injection attack scenario in cloud

2. Cross Site Scripting Attack(XSS)

XSS deals with injecting code into data context of HTML based documents at client and gaining access to sensitive information from server. It allows an attacker to execute scripts in victims' web browser. OWASP classifies XSS attacks as stored and reflected. According to the WHID (2011), 12.58% of the overall attacks on the web are associated with XSS. The variety of attacks based on XSS is almost limitless.

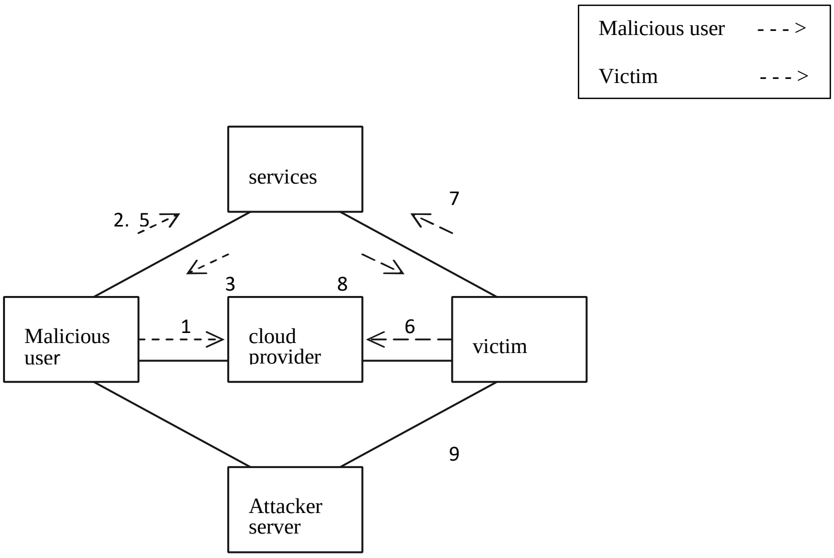

Fig. 3.A.2 Cross site scripting attack scenario in cloud

3. Command Injection Attack

Command injection is a type of code injection where the commands are injected in identified vulnerable applications. It allows such inputs to get executed on shell or in the respective runtime environment. The injected commands like ls, ps, cat etc. get executed in the runtime environment with the same privileges that a targeted application possess. One of the major consequences of the above attack is increased waiting time for the other users who makes use of applications running on the same VM in which vulnerable application runs.

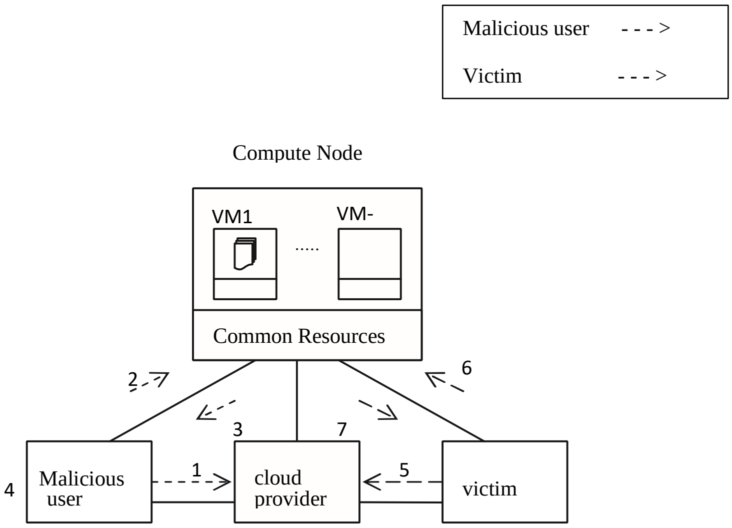

Fig. 3.*A*.3. Command injection attack scenario in cloud

4. CONCLUSION & FUTURE WORK

Vulnerabilities in web applications enable unauthorized access to cloud. Even a minute vulnerability in any one of the applications may result in a security breach of other multitenant services on cloud. Hence effective security mechanisms play vital role. Researchers continue to develop new technologies to improve the security of cloud computing. In this paper various network security issues like data breaches, account hijack, XML signature wrapping attack, malware injection and Insecure APIs have been discussed. Various research have been done in all these security issues to overcome this. In order to protect cloud computing technologies of detection, prevention and responding various attack must be developed.

REFERENCES

[1] Juraj Somorovsky, Mario Heiderich, Nils Gruschka, Luigi Lo Iacono, "All Your Clouds are Belong to us– Security Analysis of Cloud Manage- ment Interfaces" CCSW'11, October 21, 2011, Chicago, Illinois, USA.

[2] Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, Jörg Schwenk ,"Scriptless Attacks Stealing the Pie Without Touching the Sill" CCS'12,North Carolina, USA.

[3] Oracle Developers,"An Introduction to SQL Injection Attacks for Oracle Developers" March 2007.

[4] OWASP. "Command Injection"https:// www.owasp.org/ index.php/ Command_Injection.

[5] Sophos security threat report 2012, accessed on http://www.sophos.com/ medialibrary/PDFs/other/Sophos SecurityThreatReport2012.pdf

[6] [10]Hanqian Wu, Yi Ding, Chuck Winer and Li Yao, "Network Security for Virtual Machine in Cloud Computing", Computer Sciences and Convergence Information Technology (ICCIT), December 2010.

[7] TulasiRam N, Anusha K and Mary SairaBhanu S, "An Analysis of Malware Injection Attacks and Their Impact on Cloud", Engineering Sciences International Research Journal, 2330 – 4338, Volume 1, Issue 1, February-2013.

[8] S. Subhashini and V. Kavitha, "A survey on security issue in service models of cloud computing", Journal of Network and Computer Applications, July-2010.

[9] Ajey Singh and Dr. ManeeshShrivastava, "Overview of Attacks on Cloud Computing", International Journal of Engineering and Innovative Technology (IJEIT) ,Volume 1, Issue 4, April 2012.

[10] Kandias M., Virvilis N., Gritzalis D. (2013) The Insider Threat in Cloud Computing. In: Bologna S., Hämmerli B., Gritzalis D., Wolthusen S. (eds) Critical Information Infrastructure Security. CRITIS 2011. Lecture Notes in Computer Science, vol 6983. Springer, Berlin, Heidelberg

[11] KrešimirPopović andŽeljkoHocenski, "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of the 33rd International Convention, June 2010.

[12] KaziZunnurhain and Susan V. Vrbsky, "Security Attacks and Solutions in Clouds", 2010.

[13] Naveen Sharma, Dimple Malik and Mahesh Kr. Saini, "Overcoming Network Security Issues in Cloud Computing and its Applications", International Journal of Computer Applications, 2012

[14] Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, JörgSchwenk ,"Scriptless Attacks Stealing the Pie Without Touching the Sill" CCS'12,North Carolina, USA.