CLOUD COMPUTING

CHALLENGES AND SOLUTIONS

Nidal M. Turab[1] , Anas Abu Taleb [2] Shadi R. Masadeh[3]

[1,2] Department of Computer Science, Isra University, Amman, Jordan
Nedalturab@ipu.edu.jo, Anas.taleb@ipu.edu.jo
[3] Department of Computer Science, Al-Hussein Bin Talal University, Maan, Jordan
sh_almasadeh@ahu.edu.jo

ABSTRACT

Cloud computing is an emerging area of computer technology that benefits form the processing power and the computing resources of many connected, geographically distanced computers connected via Internet. Cloud computing eliminates the need of having a complete infrastructure of hardware and software to meet users requirements and applications. It can be thought of or considered as a complete or a partial outsourcing of hardware and software resources. To access cloud applications, a good Internet connection and a standard Internet browser are required. Cloud computing has its own drawback from the security point of view; this paper aims to address most of these threats and their possible solutions.

KEYWORDS

Cloud computing, integrity, privacy, cloud service provider and cloud security.

1. INTRODUCTION

Cloud computing provides its user with many capabilities like accessing a large number of applications without the need for having a license, purchasing, installing or downloading any of these applications. It also reduces both running and installation costs of computers and software as there is no need to have any infrastructure. Users can access information anywhere; all they need is to connect to a network (usually the Internet).
Cloud computing offers companies an increased storage than traditional storage systems. Software updates and batches are highly automated with reduced number of hired highly skilled IT personnel.[2], [7]
Cloud computing can be divided according to deployment models and according to service delivery models which can be found in the following subsections.

1.1 Cloud Deployment Models

There are four types of cloud computing deployment models:

- **Private cloud**: The cloud is managed by an organization and serve it solely ; it can exist inside or outside the organization's perimeter .
- **Community cloud**: The cloud is managed by several organizations and supports a specific community that has the same interest.
- **Public cloud**: The cloud infrastructure is owned and managed by a large Cloud Service Provider (CSP).
- **Hybrid cloud** – The cloud infrastructure is composed of two or more of the above models (e.g. Private and public, private and community)

1.2 Cloud computing service delivery models

Cloud computing providers offer three fundamental service models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS):

- **Infrastructure as a service (IaaS)**: Cloud computing providers offer physical and virtual computers, extra storage networking devices etc. The virtual machines are run by hypervisors that is organized into pools and controlled by operational support systems. It is cloud users responsibilities to install operating system images on the virtual machines as well as their application software.
- **Platform as a service (PaaS):** refers to computing platforms such as web servers, databases operating systems and programming environments, where the cloud user uses a software or platforms offers by CSP.
- **Software as a Service (SaaS):** Cloud users can use software that is already installed and running on the cloud infrastructure. Thus, eliminating the need of installing and running the software on their own computers. Additionally, the need for software maintenance and support is eliminated.

The main concern of the cloud computing users is the security of the information stored or transmitted to/from the cloud. In this paper we will illustrate basic cloud computing security concerns and their possible solutions.

1.3 Related work:

Several studies have been carried out regarding security issues in cloud computing from several points of view. Jarabek[6] presented an overview of the benefits and drawbacks of virtualization in a cloud context . Also he examined the side-channel information leaks which are particularly critical in a virtualized cloud environment and the Issues of security auditing and cloud management. Ian Foster[15] compared cloud computing with grid computing from various insights; Cong [8] proposed a scheme of integration of storage correctness insurance and data error localization. The proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks. Rohit [4] discussed various security concerns for Cloud computing environment from network, application and data storage perspectives and suggested some of their solutions. This paper presents a survey of the cloud computing attacks from different levels such as cloud Security Provider (CSP) level, network level and finally end user level. Additionally security attacks mitigation is also discussed in this paper.

2. CLOUD SECURITY ATTACKS

Cloud computing involves three parties: Cloud Customer or user, Cloud Service Provider CSP and Cloud network (usually the Internet that can be considered as the transmission media of the cloud) as illustrated in figure 1.

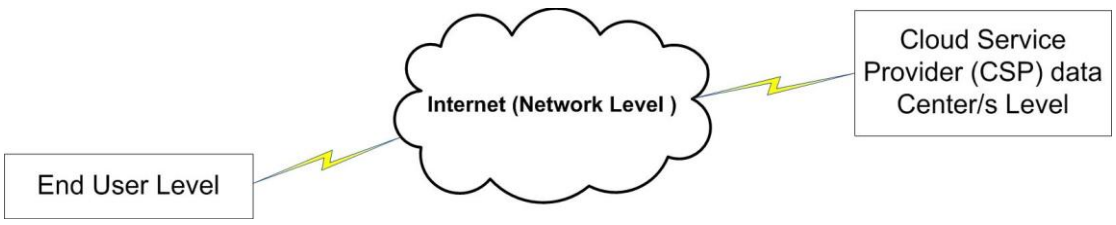

Figure 1 The three parties of cloud computing

There are many security threats at different levels, such as threats at Cloud Service Provider CSP level, network Level and user/host level. These threats must be dealt with since it is necessary to keep the cloud up and running continuously. In this section we will study different types of attacks at different levels and the ways to reduce their damage of effect.

2.1 Cloud Service Provider CSP level attacks

The shared nature of the cloud and the increased demand on shared resource of the cloud computing could be an attractive target to attackers. End users should take into consideration the vulnerabilities of cloud computing before migrating to it. Examples of shared resources are computing capacity, storage, and network [3]; this shared nature exposes the cloud to many security breaches that are listed below:

2.1.1 Guest-hopping attack: is defined as any separation failure between shared infrastructures. An attacker will try get access to one virtual machine by penetrating another virtual machine hosted in the same hardware. One of the possible mitigations of guest hopping attack is the Forensics and VM debugging tools to observe any attempt to compromise VM. [3] Another possible mitigation is using **High Assurance Platform (HAP)** which provides a high degree of isolation between virtual machines.

2.1.2 SQL injection: is often used to attack websites. It is accomplished by injecting SQL commands into a database of an application from the web to dump or crash that database. To mitigate SQL injection attack; it is necessary to remove all stored procedures that are rarely used. Also, assign the least possible privileges to users who have permissions to access the database. [4]

2.1.3 Side channel attack: is when the attacker places a malicious virtual machine on the same physical machine as the victim machine; in that way the attacker can access all the confidential information on the victim machine.

As a countermeasure, it might be preferable to ensure that none of the legitimate user VMs resides on the same hardware of other users. This completely eliminates the risk of side-channel attacks in a virtualized cloud environment. [5], [6].

2.1.4 Malicious Insider: One of the cloud computing challenges located at the data centers of the service providers is when its employee is granted access to sensitive data of some or all customers administrators. Such system privileges can expose these information to security threats. Strict privileges' planning, security auditing can minimize this security threat [7].

2.1.5 Data storage security

In cloud computing, user's data is stored in the Cloud Service Provider (CSP) set of servers, which are running in a simultaneous and distributed manner. Ensuring data integrity and confidently is vital. According to [8],[9],[16] there are some means to ensure integrity and confidently of the data stored at the CSP that are listed below.

1. Ensure limited access to the users' data by the CSP employees.
2. Strong authentication mechanisms to ensure that only legitimate employees gain access and control CSP servers.
3. The CSP should use well defined Data backup and redundant data storage to make data recovery possible.

2.1.6 Address Resolution Protocol (ARP) Cache Poisoning

Address Resolution Protocol **(**ARP) is used in the TCP/IP stack to resolve an IP address (logical) at the sender side into MAC address (physical) address at the receiver side. The ARP

cache stores a table that maps all the IP address of the networked devices and their corresponding MAC addresses. An attacker can exploit some weakness in the ARP protocol to map an IP address of the network to one malicious MAC, and then update the ARP cache with this malicious MAC address. To mitigate this attack it is possible to use static ARP entries, this technique can work for small networks like private clouds; but on large scale clouds it is better to use other techniques such as port security features that locks a specific port on the switch (or network device) to a specific IP address [10].
It should be noticed that CSP must have the latest network security enhancement techniques such as Firewalls, Intrusion Detection/Prevention techniques, Centralized antivirus and anti-malware techniques that runs multi antivirus solutions simultaneously to ensure best virus and malware protection. Another important issue is to use IPSEC/VPN techniques between the CSP and cloud users whenever it is possible. In addition, high physical security at the CSP data center/s is vital, physical data security includes: Access control only for authorized personnel, special fire systems, very specific data storage and backup strategists, etc.

2.2 Network Level Security attacks

Cloud computing depends mainly on the existing networks infrastructure such as LAN, MAN and WAN; that is why cloud computing is exposed to the same security attacks. These attacks may be originated from users outside the cloud (a user intended to attack the cloud for any purpose), or a malicious insider residing between the user and the CSP and trying to interrupt the data to/from the cloud. In this section we will try to focus on the network level security attacks and their possible countermeasures to insure proper data confidentiality and integrity.

2.2.1 Domain Name System (DNS) attacks

In the Internet, hosts are defined by names that are easy to remember by humans, while computers deal with numbers. Each connected computer to the Internet has a globally unique Internet Protocol (IP). The Domain Name System (DNS) converts host names into corresponding Internet Protocol (IP) addresses using a distributed database scheme. Internet DNS servers are subject to different types of attacks such as: ARP cache poisoning (as explained in 3.1.6), domain hijacking, and man-in-the-middle attacks. A discussion of these attacks can be found below.

2.2.2 Domain hijacking

Domain hijacking is defined as changing the name of a domain without the knowledge or permission from the domain's owner or creator. Domain hijacking enables intruders to access sensitive corporate information and perform illegal activity such as phishing, where a website is replaced by an identical website that records private information. One of the possible ways to make domain hijacking very difficult is proposed by Internet Corporation for Assigned Names and Numbers (ICANN) which forces a 60-day waiting period between a change in registration information and a transfer to another registrar; most likely that the domain creator will discover any change in that period. Another solution is using Extensible Provisioning Protocol (EPP) that is used by many domain registries. EPP uses an authorization code issued exclusively to the domain registrant as a security measure to prevent unauthorized name changing. [21]

2.2.3 IP Spoofing

IP spoofing is where the attacker gains unauthorized access to a computer by pretending that the traffic has originated form a legitimate computer. IP spoofing is utilized to make other attacks such as Denial of Service attack and Man in The Middle attack: [12]

Denial of service attacks (DoS): The purpose of these attacks is making the target network/computer resources unavailable. In DoS attack the attacker floods the victim host with a huge number of packets in a short amount of time, DoS is concerned only with consuming

bandwidth and resources of the target network/computer. The attacker uses a spoofed IP address as the source IP address to make tracking and stopping of Dos very difficult. Furthermore, it is possible to the attacker to use multiple compromised machines which he has already hijacked to attack the victim machine at the same time (this attack is known as Distributed DoS) and it is very difficult to track and stop.

TCP SYN flooding is an example of DoS attack; the attacker floods the victim machine with a stream of spoofed TCP SYN packets. This attack exploits the limitations of the three way handshake in maintaining half-open connections.

Man In The Middle Attack (MITM): An attacker gains access to the network traffic using network packet sniffer, routing and transport protocols flaws, these attacks could be used for theft of confidential information. [10]
IP spoofing can be reduced using packet filtering by firewall, strong encryption and origin authentication techniques.

2.3 End users' attacks

Most of the cloud users' attacks are phishing, fraud, and exploitation of software vulnerabilities still work and can threaten the cloud service infrastructure. [17]

Phishing and fraud: are attempts to steal the identity of a legitimate user such as usernames, passwords, and credit card details. Phishing is typically carried out by sending the user an email that contains a link to a fraud website that looks like a legitimate one, when the user goes to that fake website, his user name and password will be sent to the attacker who can use them to attack the cloud. Another form of phishing and fraud is to send the user an email that pretends to become from the cloud service provider and asking the user to supply his username and password for maintenance purposes for example; but indeed that spoofed email came from an attacker to gain the user credentials then using them to attack the cloud. Countermeasures of phishing are the use of Spam-filters, using plug-in spam blocker in the Internet browsers and finally train the users not to respond to any spoofed email and not to give their credentials to any website.

Exploitation of software vulnerabilities: is any security flaw or weakness that can be found in an operating system or a software that leads to security breach. This security breach is used by an attacker to implant a malware for his own purpose [18], [19]. Common example of this attack is buffer overflow where the operating system or software hangs and uncontrolled format string that can be used to crash a program or to execute malicious code. Software vendors regularly release security updates to address these flaws; updating systems with the latest security updates can mitigate these attacks.

3. Conclusions

Cloud computing is an emerging technology. It is an attractive solution when the infrastructure or the IT personnel are not available or too expensive; but it has its drawback. The drawback can be mainly found in the security threats and vulnerabilities of the cloud computing. Unlike traditional solutions where threats come from two known sources inside or outside the network; cloud computing security threats might originate from different sources. In this paper we discussed most of the cloud security threats from three prospective levels: application, network and user levels. Also we address some possible ways to reduce security as possible.

References

1. [1] “Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0”, https://cloudsecurityalliance.org/research/security-guidance/
2. “IT-3_Cloud_Computing” A news Letter for IT professionals Issue 3 2012
3. Center Of Protection Of National Infrastructure Information Security Briefing cloud-computing-briefing.pdf.
4. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki” A Survey on Security Issues in Cloud Computing” http://arxiv.org/ftp/arxiv/papers/1109/1109.5388.pdf
5. Imperia Data Security Hacker Intelligence Initiative, Monthly Trend Report #4 report http://blog.imperva.com/2011/09/sql-injection-by-the-numbers.html
6. Christopher Jarabek “Virtualization, Side-Channel Attacks, and Management http://blog.imperva.com/2011/09/sql-injection-by-the-numbers.html
7. Cloud security alliance “Security guidance for critical areas of focus in cloud computing V3.0” https://cloudsec_urityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/
8. Cong Wang, Qian Wang, and Kui Ren” Ensuring Data Storage Security in Cloud Computing” http://ieeexplore.ieee.org/xpl/login.jsp ?tp=&arnumbe r=5201385&url= http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5201378%2F5201379%2F05201385.pdf%3Farnumber%3D5201385, 2009.
9. Rohit Bhadauria, Rituparna Chaki “A Survey on Security Issues in Cloud Computing” international journal of computer applications Volume 47 - Number 18.2012
10. “ Amazon Web Services: Overview of Security Processes” http://aws.amazon.com, 2009.
11. Ruiping Lua and Kin Choong Yow, “Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network,” IEEE Network, vol. 25, no. 4, 2011.
12. B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference onServices Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. 2009. ISBN: 978-0-7695-3811-2
13. Tanase, Matthew “2003). "IP Spoofing: An Introduction” The Security Blog. Retrieved February 10, 2012.
14. Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, “A Cooperative Intrusion Detection System Framework for Cloud Computing Networks,” ICPPW ’10 Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society, pp. 280-284, Washington DC, USA, 2010. ISBN: 978-0-7695-4157-0.
15. Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu” Cloud Computing and Grid Computing 360-Degree Compared” http://arxiv.org/ ftp/arxiv/papers /0901 /0901.0131.pdf
16. Rajnish Choubey, Rajshree Dubey, Joy Bhattacharjee “A Survey on Cloud Computing Security, Challenges and Threats” International Journal on Computer Science and Engineering (IJCSE)
17. Klaus Pl¨ossl, Hannes Federrath, and Thomas Nowey “Protection Mechanisms against Phishing Attacks” http://www-sec.uni-regensburg.de/publ/2005/ PlFN2005Trust Bus05Phishing.pdf
18. Wright, Joe; Jim Harmening “*Computer and Information Security Handbook*.” Morgan Kaufmann Publications. Elsevier Inc. p. 257. ISBN 978-0-12-374354-1
19. Bavisi, Sanjay (2009). "22". *Computer and Information Security Handbook*. Morgan Kaufmann Publications. Elsevier Inc. p. 375. ISBN 978-0-12-374354-1
20. Domain name hijacking: Incidents, threats, risks, and remedial action. A report from the ICANN Security and Stability Advisory Committee (SSAC) 2005
21. RFC 3375 “Generic Registry-Registrar Protocol Requirements”; http://tools.ietf.org/pdf/rfc3375.pdf.

Authors

Dr. Nidal Turab *received a BSc degree incommunication engineering from theUniversity of Garounis, Benghazi, libya 1992 and an MSc in telecommunicationengineering from the University of Jordan,Amman in 1996. His PhD in computerscience is from the Polytechnic Universityof Bucharest, 2008. His research interests include WLAN security, computer network security and cloud computing security.. He is an assistant professor at Isra University.*

Dr. Anas Abu Taleb*: is an assistant professor in the department of Computer Science at Isra University, Amman, Jordan. He received a Ph.D. in Computer Science from the University of Bristol, UK, 2010, MS.c. in Computer Science from the University of the West of England, UK, 2007 and BS.c. degree in Computer Science from Princess Sumaya University for Technology, Jordan, 2004. Dr. Abu Taleb has published several journal and conference papers in sensor networks. In addition to sensor networks, Dr. Abu Taleb is interested in sensor networks, network fault tolerance, routing algorithms, and cloud computing.*

Shadi R. Masadeh *received a BSc degree in Computer Science and Computer Information System in 2000 and MSc degree in Information Technology in 2003. with a Thesis titled "A Mathematical Approach for Ciphering and Deciphering Techniques" After that, I received PhD from department of Computer Information System in 2009 with a Thesis titled "A New Embedded Method for Encryption/Decryption Technique Using Self Approach" My research interests including E-learning Management and Security Issues, Encryption and Decryption Systems. Networking and Wireless security. Currently, I'm working at Al-Hussein Bin Talal University in Computer Science Department as assistant Prof. I have submitted a number of conference papers and journals.*