Challenges Of Security Issues In Cloud Computing Layers

Amin Panah[1] , Amir Panah[2] , Omid Panah[3] and Samere Fallahpour[4]

[1]*Department of Computer, Islamic Azad University, Yazd Branch, Yazd, Iran*
[2]*Faculty Member of Computer and IT Department, Hadaf Higher Education Institute, Sari, Iran*
3Faculty Member of Computer Department, Islamic Azad University, Ayatollah Amoli Branch, Amol, Iran
[4]*Mazandaran University of Medical Sciences, Sari, Iran*
e-mail: amin.panah2020@gmail.com, a.panah@hadaf.ac.ir,
o.panah@iauamol.ac.ir,samere.fallahpour@gmail.com

Abstract. Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges. In this article, we focus on security in some layer of cloud computing, which has always been an important aspect of quality of service.
[Amin Panah; Amir Panah; Omid Panah;Samere Fallahpour. **Challenges Of Security Issues In Cloud Computing Layers.** *Rep Opinion* 2012;4(10):25-29]. (ISSN: 1553-9873). http://www.sciencepub.net/report.7

Keywords: Cloud computing, Securiyt Problem, Attacks, Layers.

1. Introduction

With a long-term accumulation of information technologies, cloud computing becomes a new revolution after the personal computer (PC) revolution in 1980s, the Internet revolution in 1990s, and the mobile Internet revolution in 2000s. Cloud computing is a paradigm of Internet computing in which users ever changing personalized requirements could be satisfied by software as a service in a manner of on-demand services. Cloud computing is now changing the way we share data, information, and knowledge. The benefits of cloud computing are many. One is reduced cost, since you pay as you go. Other benefits are the portability of the application is that users can work from home, work, or at client locations. This increased mobility means employees can access information anywhere they are. The public are now enjoying the capabilities of super-computing and mass storage provided by cloud computing, but the security problem of cloud computing becomes a hot spot issue.

2. Different models and layers of cloud computing

2.1. Models

To continue, we study four existing model of cloud computing (public clouds, Private Cloud, Community Cloud, Hybrid Cloud).

2.1.1. Public clouds

A cloud infrastructure is provided to many customers and is managed by a third party. Multiple enterprises can work on the infrastructure provided, at the same time. Users can dynamically provision resources through the internet from an off-site service provider. Wastage of resources is checked as the user pays for whatever they use[7].

2.1.2. Private clouds

All of these services are deployed through a privately owned data center used exclusively by the organization that builds it. These private clouds may deploy proprietary technologies inaccessible to other users of cloud services[3].

2.1.3. Community clouds

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise[10].

2.1.4. Hybrid clouds

Which focus primarily on proprietary data centers, but rely on public cloud resources to provide the computing and storage needed to protect against unexpected or infrequent increases in demand for computing resources[3].

2.2. Layers of Cloud Computing Model

There are five layers in cloud computing model, the Client Layer, Application Layer, Platform layer, Infrastructure layer and server layer.

2.2.1. Client Layer

The cloud client consist of the computer hardware and the computer software that is totally based on the applications of the cloud services and basically designed in such way that it provides application delivery to the multiple servers at the same time, as some computers making use of the various devices which includes computers, phones, operating systems, browsers and other devices[7].

2.2.2. Application Layer

The Cloud application services deliver software as a service over the internet for eliminating the need to install and run the application on the customer own computers using the simplified maintenance and support for the people which will use the cloud interchangeably for the network based access and management of the network software by controlling the activities which is managed in the central locations by enabling customers to access the applications remotely with respect to Web and application software are also delivered to many model instances that includes the various standards that is price, partnership and management characteristics which provides the updates for the centralize features[7].

2.2.3. Platform Layer

Offers an operating system as well as suites of programming languages and software development tools that customers can use to develop their own applications. Prominent examples include Microsoft Windows Azure and Google App Engine. PaaS gives end users control over application design, but does not give them control over the physical infrastructure[3].

2.2.4. Server Layer

Offers end users direct access to processing, storage, and other computing resources and allows them to configure those resources and run operating systems and software on them as they see fit. Examples of IaaS include Amazon Elastic Compute Cloud (EC2), Rackspace, and IBM Computing on Demand[3].

3. BARRIERS TO CLOUD COMPUTING

3.1. Security

Security is typically ranked the top cloud computing adoption concern. Key threats include: abusive and nefarious usage; insecure interfaces and APIs; malicious insiders; shared technology issues; data loss or leakage; account or service hijacking, and; general uncertainty due to 'security by obscurity'[15].

3.2. Performance, Latency and Reliability

Latency has always been an issue in cloud computing with data expected to flow around different clouds. The other factors that add to the latency are encryption and decryption of the data when it moves around unreliable and public networks, congestion, packet loss and windowing. Congestion adds to the latency when the traffic flow through the network is high and there are many requests (may be of same priority) that need to be executed at the same time. Windowing is another message passing technique whereby the receiver has to send a message to the sender that it has received the earlier sent packet and hence adds to the network latency. Moreover, the performance of the system is also a factor that should be taken into account. Sometimes the cloud service providers' run short of capacity either by allowing access to too many virtual machines or reaching upper throughput thresholds on their Internet links because of high demand arising from the customer section. This hurts the system performance and adds to latency of the system[15].

3.3. Lock-in

This category combines several critical risks with characteristics that could be positioned along a spectrum spanning fully proprietary through to standardized services. They include vendor lock-in, technology lock-in, migration, interoperability, architecture, licensing and standards. Due to the rapid emergence of cloud computing through the initiatives of individual companies, most offerings are highly proprietary in nature. This creates challenges in migrating data and applications to the cloud, or switching cloud providers, and puts customers at significant risk if the need arises for systems to interoperate across cloud and in-house environments or to retrieve data and/or applications if a cloud provider withdraws from the market[15].

3.4. Data-Breach through Fibre Optic Networks

It has been noticed that the security risks for the data in transit has increased over the last few years. Data transitioning is quite normal now-a-days and it may include multiple data-centres and other cloud deployment models such as public or private cloud. Security of the data leaving a data-centre to another data-centre is a major concern as it has been breached quite a number of times in the recent times. This data transfer is done over a network of fibre-optic cables which were considered to be a safe mode of data-transfer, until recently an illegal fibre

eavesdropping device in Telco Verizon's optical network placed at a mutual fund company was discovered by US Security forces[15].

4. Threats In Layers Of Cloud Computing

In this part of our article we study some existing THREATS in two layers of cloud computing, application and network, and their cost for them. To continue, we study approach for solve or avoid from that threats.

4.1. Application Level Attackts

4.1.1. Denial Of Service Attacks

Denial of service attacks are easier in an environment with such a high number of users if not appropriately manager. Thus, workload management to control cloud scalability in massively used datacenters is a pending security issue. In the cloud, administrative access is done via the Internet rather than the restricted on-premises connection in the traditional data center model. This increases risk, thus requiring more demanding monitoring for changes in system control and access control restriction and increases bandwidth consumption besides causing congestion, making certain parts of the clouds inaccessible to the users[9].

4.1.2. Cookie Poisoning

It involves changing or modifying the contents of cookie to make unauthorized access to an application or to a webpage. Cookies basically contain the user's identity related credentials and once these cookies are accessible, the content of these cookies can be forged to impersonate an authorized user[15].

4.1.3. Hidden Field Manipulation

When we fill in some information and press the submit button, a confirmation screen uses the value of the userID hidden field from the HTML form. A hacker can use the browser's ''Save as'' feature to save the HTML of the change address form to his/her computer. The complete HTML, including values in the hidden fields are saved. Then he/she can open the HTMLfile with a text editor and change the userID field and save the file. And then he/she can alter the other hidden fields as well. Thus he/she can open the file in his/her web browser and submit the form.As the application is trustworthy with respect to its contents of the hidden fields, any user knowledgeable enough to save and load the HTML is able to alter the userID field and make changes freely to the addresses of any user they like. Checking HTTP_REFERER will catch trivial attempts to tamper with forms, but cannot be relied on for serious web applications[9].

4.1.4. Malicious Insider

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[9].

4.2. Network Level Attacks

Some possible attack exist In network layer that we explain them and offer some Approach for solve them.

4.2.1. Dns Attaks

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible[16].

4.2.2. Sniffer Attacks

These types of attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network[16].

4.2.3. Malware-Injection Attack

In the cloud system, as the client's request is executed based on authentication and authorization, there is a huge possibility of meta data exchange between the web server and web browser. An attacker can take advantage during this exchange of metadata. Either the adversary makes his own instance or the adversary may try to intrude with malicious code. In this case, either the injected malicious service or code appears as one of the valid instance services running in the cloud. If the attacker is successful, then the

cloud service will suffer from eavesdropping and deadlocks, which forces a legitimate user to wait until the completion of a job which was not generated by the user. This type of attack is also known as a meta-data spoofing attack[17].

4.3. Approachs For Defence Against Attacks

4.3.1. DOS Attack Solution

Using an Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks. Each cloud is loaded with separate IDS. The different intrusion detection systems work on the basis of information exchange. In case a specific cloud is under attack, then the co-operative IDS alert the whole system[9].

4.3.2. Cookie Poisoning Attack Solution

This can be avoided either by performing regular cookie cleanup or implementing an encryption scheme for the cookie data[15].

4.3.3. Hidden Field Manipulation Attack Solution

Experienced web HTTP_REFERER variable. Most browsers send an HTTP header named ‘‘HTTP_REFERER’’. It contains programmers believe that this type of tampering can be easily prevented by checking the the URL of the page the user viewed before the current one. If the hacker saves the form to his/her computer and resubmits it, HTTP_REFERER is blank or contains a different URL. This is not a safe method to validate a form against tampering. Just like form fields, the value of HTTP_REFERER is set by the web browser. A user with only a little knowledge can write a script to spoof this header along with the contents of the form. Checking HTTP_REFERER will catch trivial attempts to tamper with forms, but cannot be relied on for serious web applications[9].

4.3.4. Malicious Insider Attack Solution

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[9].

4.3.5. DNS Attack Solution

Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems[16].

4.3.6. Sniffer Attack Solution

A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network[16].

4.3.7. Malware-injection Attack Solution

The client’s VM is created and stored in the image repository system of the cloud. These applications are always considered with high integrity. We propose to consider the integrity in the hardware level, because it will be very difficult for an attacker to intrude in the IaaS level. Our proposal is to utilize a FAT-like (File Allocation Table) system architecture due to its straightforward technique which is supported by virtually all existing operating systems. From this FAT-like table we can find the application that a customer is running. A Hypervisor can be deployed in the provider’s end. The Hypervisor is responsible for scheduling all the instances, but before scheduling it will check the integrity of the instance from the FAT-like table of the customer’s VM[17].

5. Conclusion

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. Moreover data residing in the cloud is also prone to a number of threats and various issues like confidentiality and integrity of data should be considered while buying storage services from a cloud service provider. In this paper various security concerns in two layers of Cloud computing and the solutions to prevent them have been presented[15].

In the future, we will extend our research by providing implementations and producing results to justify our concepts of security for cloud computing. The concepts we have discussed here will help to build a strong architecture for security in the field of cloud computation. This kind of structured security will also be able to improve customer satisfaction to a great extent and will attract more investors in this cloud computation concept for industrial as well as future research farms. Lastly, we propose to build strong theoretical concepts for security in order to build a more generalized architecture to prevent different kinds of attacks[17].

6. References

1. Ajith Singh. N,Vasanthi.V , and M. Hemalatha.: A Brief Survey on Architecture, Challenges & Security Benefit in Cloud Computing. International Journal of Information and Communication Technology Research. Volume 2 No.2. (2012)
2. B. R. Kandukuri, R. V. Paturi and A. Rakshit.: Cloud Security Issues. IEEE International Conference on Services Computing, Bangalore, India, In Proceedings of IEEE SCC'2009. pp. 517-520. (2009)
3. Christopher S. Yoo.: Cloud Computing: Architectural and Policy Implications. Springer Science+Business Media Published online. (2011)
4. Cong Wang, Qian Wang, and Kui Ren.: Ensuring Data Storage Security in Cloud Computing. Department of ECE. Illinois Institute of Technology. (2010)
5. D. Gollmann.: Securing Web Applications. Information Security Technical Report. Elsevier Advanced Technology Publications Oxford, UK, vol. 13, issue. 1. (2008)
6. E. B. Dudin, and Yu. G. Smetanin. :A Review of Cloud Computing. Scientific and Technical Information Processing, Vol. 38, No. 4, pp. 280–284. (2011)
7. Jeon Seung Hwan, Yvette E, Gelogo and Byungjoo Park.: Next Generation Cloud Computing Issues and Solutions. International Journal of Control and Automation Vol. 5, No.1. (2012)
8. Luis M.Vaquero, Luis Rodero-Merino, Daniel Moran:. Locking the sky: a survey on IaaS cloud security. Published online: © Springer-Verlag (2010)
9. Mervat Adib Bamiah, and Sarfraz Nawaz Brohi.: Seven Deadly Threats and Vulnerabilities in Cloud Computing. INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES VOL No. 9, Issue No. 1. (2011)
10. Meiko Jenson, Jorg Schwenk, Nils Gruschka, and Luigi Lo Iacono.: On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing. (2009)
11. . Michael Armbrust. Armando Fox. Rean Griffith. Anthony D. Joseph Randy H. Katz. Andrew Konwinski. Gunho Lee and David A.: Patterson Ariel Rabkin Ion Stoica Matei Zaharia.Above the Clouds. A Berkeley View of Cloud Computing UC Berkeley Reliable Adaptive Distributed Systems Laboratory, http://radlab.cs.berkeley.edu/ February 10. (2009)
12. Rajnish Choubey, Rajshree Dubey, and Joy Bhattacharjee.: A Survey on Cloud Computing Security, Challenges and Threats. International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 3. (2011)
13. Sean Carlin, and Kevin Curran.: Cloud Computing Security**.** 14International Journal of Ambient Computing and Intelligence, 3(1). (2011)
14. Meiko Jenson, Jorg Schwenk, Nils Gruschka, and Luigi Lo Iacono.: On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing. (2009)
15. Sugata Sanyal, Nabendu Chaki, Rituparna Chaki, and Rohit Bhadauria:. A Survey on Security Issues in Cloud Computing. the IEEE Communications Surveys and Tutorials (2011)
16. Suresh Chandra Satapathy, Manas Ranjan Patra, Rabi Prasad Padhy:. Cloud Computing: Security Issues and Research Challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December (2011)
17. Susan V. Vrbsky, Kazi Zunnurhain:. Security in Cloud Computing. International Conference on Security & Management(2011)
18. Yu-Chao Liu, Yu-Tao Ma, Hai-Su Zhang, De-Yi Li, and Gui-Sheng Chen:. A Method for Trust Management in Cloud Computing: Data Coloring by Cloud Watermarking. International Journal of Automation and Computing 8(3)(2011)

9/10/2012