Personal Security in the Application of Online Software in the Technology Period 4.0

Nguyen Tan Danh

FPT University, Vietnam
Email: nguyentandanh0774@gmail.com

***Article History**: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021*

ABTRACT

Over the three industrial revolutions, man has achieved great achievements. But besides that great success will always go hand in hand with many problems that arise. Because the rate at which technology develops is directly proportional to the threats it poses. The emergence of new technology requires researchers and students to pay attention to discover new threats to make it reliable and user-friendly. In the meantime 4.0 cloud computing is a new technology model. Security issues in cloud computing are considered one of the biggest obstacles besides the broad benefits of cloud computing. New concepts introduced by the cloud create new challenges for the security community. Addressing these challenges requires, in addition to the ability to cultivate and adjust security measures developed for other systems, to propose new security policies, models and protocols to address optimal and effective cloud security challenges. In this article, we provide comprehensive research on cloud security including classification of known security threats and advanced practices in attempting to address these threats. The paper also provides classification dependency and provides solutions in the form of preventive action rather than proactive action.

Keywords: achievements, cloud computing, industrial revolutions

1. INTRODUCTION

In the development era of Industry 4.0, people have step by step researched and developed and achieved outstanding achievements. But besides the development of technology, there is always a shortcoming, especially the issue of user security and security in the current digital wait. In which, cloud computing technology is a broad model, based on the software and hosting service provisioning model as the foundation. The concept of cloud computing has emerged from the fields of distributed computing and the mesh has been used for servers, in web hosting, and hosting services. Cloud computing, as defined by NIST, is called: A model that allows universal, convenient on-demand network access, into a group of configurable computing resources (e.g. network, machine servers, storage, applications, and services) may be promptly available and released with minimal administrative effort or service provider interaction [1].

2. LITERATURE REVIEW

The application software at SaaS is provided with a subscription based on a specific license, pay-as-you-go [2]. Platform is a service (PaaS) that serves operating system, network capacity, storage, and multi-tenancy services over the Internet. Infrastructure as a Service (IaaS) provides compute utility, automation of administration tasks, dynamic replication, desktop virtualization, policy-based services, and Internet connectivity. IaaS provides virtual server with unique IP address and hosting group according to customer's requirement. The concept of infrastructure and hardware layer is mentioned by different researchers. Some authors argue that the infrastructure layer provides the system software services and the hardware layer provides the services based on the hardware. The infrastructure and hardware layers can be combined due to the intrinsic relationship between hardware and software.

The security aspects of one of the popular Amazon Elastic Compute Cloud (EC2) cloud have been discussed [4]. It includes systematic analysis of various critical vulnerabilities in publicly available Amazon Machine Images (AMIs) and mechanisms for their elimination. The proposed tool called the Amazon Image Attack (AmazonIA) uses only publicly available interfaces regardless of the underlying cloud infrastructure. Due to the successful exploit and attack, the authors are able to extract sensitive information including passwords and credentials from AMI. The extracted information can be used to initiate a botnet or create a backdoor to launch impersonation attacks or access the source code of a web service available on the AMI. The authors discussed the effects of successful attacks and also methods to mitigate those attacks. Several research teams have been working on the interfaces of both public and private clouds [5]. The public cloud under their consideration is Amazon, while the private cloud is Eucalyptus.

Some authors consider security as a service for cloud-based applications. The architecture considers the existing services at different levels. It considers user-centric security, i.e. users have control over their security allowing them to use security solutions across different clouds. They can subscribe to any security solution offered by any cloud provider and use that particular security solution for their cloud, and can also have multiple security solutions for A particular service depends on its importance. Security solutions can also be used at different levels [6].

There are authors proposing that security should be provided as a service and proposing a model for security as a service. Security as a service implies that security applications and services can be provided by a cloud provider or cloud consumer or even by a trusted third party. Security services can be in the form of infrastructure or cloud-based software. The authors have proposed a component-based software model, in which authorized components can be developed by any party regardless of service provider. The eXtensible (XACML) access control markup language decision tool includes a context handler, policy decision point, and policy administration point, which can be provided by reusable components. to enhance security services. According to the XACML standard properties of objects, resources and the environment, and authorization rules can be defined as Boolean expressions. Therefore, these types of security services, which can be managed and modified by the cloud client, are very useful for building cloud client trust on cloud systems [7].

3. RESEARCH METHODS

Based on research from many database sources that some authors have previously studied. Plus survey data from existing community that have been using social networks like facebook, twitter or some other cloud software. In order to find out research about their feelings when using, along with the confidentiality of personal information about users of these software is guaranteed or not.

4. RESEARCH RESULTS

Cloud computing applications are deployed in a shared resource environment, so data security is a very important aspect. Data privacy has three major challenges: integrity, access, and usability (backup / copy). Data integrity ensures that data is not corrupted or tampered with during communication. Authorized access prevents data from intrusion attacks during backup and replication allowing efficient data access even in the event of a technical failure or disaster in some locations in the cloud . Data is shared and communicated at the common backbone. As a result, malicious attackers or intruders can deploy hidden proxy applications between the cloud provider and the consumer to collect login credentials. An intruder can also perform packet sniffing or IP spoofing as an intermediary and can access and / or change restricted or sensitive information. A viable solution for data privacy in the cloud is the Cisco Secure Data Center Framework, which provides a layered security mechanism [8].

A successful attack on the cloud interfaces can result in a machine's root level access without initiating a direct attack on the cloud infrastructure. Two different types of attacks are launched in the cloud. The console is vulnerable to advanced signature wrapping and cross-page scripting (XSS) techniques. The first attack is known as a signature packet attack or XML Signature Pack attack. Can SOAP messages with single signature or X.509 certificate be used to compromise client security? account through operations on virtual machines or reset the password. The second type of attack exploits a vulnerability in XSS. The vulnerability attack specifically steals username and password pair information.

Attack on Secure Shell (SSH), the basic mechanism used to establish trust and connect to cloud services, is the most alarming threat to compromise control trust. According to the 2014 Ponemon SSH Vulnerability Report, 74 percent of organizations have no control over the provision, rotation, tracking, and deletion of SSH keys. Cybercriminals make the most of these vulnerabilities and use cloud computing to launch various attacks. An organization's cloud workload can be used by the host botnet if SSH access is compromised. The attackers hosted the Zeus botnet and control infrastructure on Amazon EC2 instances. Different types of attacks on SSH include attacks on API keys, attacks on user credentials and attacks on publisher credentials [8].

The results after surveying about twenty people who are already using social networks or one of the other programs using cloud computing technology. Research on their safety attitudes and feelings during use, and the satisfaction of the users' security when using these programs.

It can be seen that the majority of people who have been using cloud computing technology are aware of the importance of protecting personal information when using these programs; others replied that they never trust the security system of these programs, some say that the program is absolutely secure and there are no problems to worry about.

5. DISCUSSION

Because cloud computing technology is used in a common environment, their security is a very important issue. But some people currently using this software do not take the security of their personal information seriously. But the program has always had holes in which other people can take advantage of them to steal your personal information.

The categorization defines the levels of risk as low (less vulnerable), medium, and high (more vulnerable) depending on the applicability of the cloud security requirements. Data encryption, multi-lease, data security, authentication, and authorization are security requirements for cloud services. These security requirements constitute different levels of risk. For example, multi-tenancy and data security for hardware virtualization present high risks when using cloud computing software.

The level of risk associated with hardware virtualization is medium to high. Cloud computing software is threatened by automated hacking tools and has a high level of risk. Malicious code and scripts can be executed with development services, and they can adversely affect the entire cloud system and thus the risk of impact associated with development services is high.

Mistakenly limiting the loss of personal information of users, cloud computing providers and developers need to be constantly updated with the latest information and security technologies. Investigate and detect holes that are or are likely to appear, find the earliest and most effective way to overcome them. Listen to the views of the people who use these services to make the right changes or to correct them when something goes wrong.

In addition to the work of cloud technology management companies and authorities, users are also responsible for protecting their own personal information. Through the steps, regularly changing the password, the password should include capital letters and numbers, and use many different passwords for multiple login accounts. Also do not log personal information such as phone, email address, bank account to suspicious websites. Log out of personal information when using shared computers. We should not let others use your personal information, immediately notify service providers and competent authorities when an incident arises to get the most timely assistance.

6. CONCLUSION

Technology is always evolving, but besides the good benefits it brings, there are always people who exploit it inappropriately. Cloud computing technology in the 4.0 era is no exception, backing up data directly on the network brings many high efficiency in working in many different fields. But putting all databases into a common system also comes with many risks, in terms of the user's confidentiality, which other people can use to access, steal sensitive information. Cloud service providers always have to improve their false security software to minimize unauthorized access and data theft, but vulnerabilities will always appear, so users should be aware and responsible for their own personal information when using the network environment and cloud computing software, social networks.

REFERENCES

[1] Cloud, H. (2011). The nist definition of cloud computing. National Institute of Science and Technology, Special Publication, 800, 145.

[2] Arora, P., Wadhawan, R. C., & Ahuja, E. S. P. (2012). Cloud computing security issues in infrastructure as a service. International journal of advanced research in computer science and software engineering, 2(1).

[3] Bugiel, S., Nürnberger, S., Pöppelmann, T., Sadeghi, A. R., & Schneider, T. (2011, October). Amazonia: when elasticity snaps back. In Proceedings of the 18th ACM conference on Computer and communications security, 389-400.

[4] Aguiar, E., Zhang, Y., & Blanton, M. (2014). An overview of issues and recent developments in cloud computing and storage security. High Performance Cloud Auditing and Applications, 3-33.

[5] Somorovsky, J., Heiderich, M., Jensen, M., Schwenk, J., Gruschka, N., & Lo Iacono, L. (2011, October). All your clouds are belong to us: security analysis of cloud management interfaces. In Proceedings of the 3rd ACM workshop on Cloud computing security workshop, 3-14.

[6] Hussain, M., & Abdulsalam, H. (2011, April). SECaaS: security as a service for cloud-based applications. In Proceedings of the Second Kuwait Conference on e-Services and e-Systems (pp. 1-4).

[7] Laborde, R., Barrère, F., & Benzekri, A. (2013, April). Toward authorization as a service: a study of the XACML standard. In Proceedings of the 16th Communications & Networking Symposium, 1-7.

[8] Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 13(1), 57-65.