Unresolved Threats in Cloud Computing

Prepared for
Prof. Christine Choi
New York City College of Technology, CUNY

Prepared by
Ronald Ezekiel Felipe
Minhajul Islam
Awais Saleem

December 15, 2020

Table of Contents

Introduction to the Study

Ronald - Introduction

Cloud Computing is one of the fastest and largest technologies evolving today. It offers many great benefits like providing remote services, storage, networks, applications and more. Its key advantages are its cost-effectiveness, high scalability, and flexibility. Additionally, Cloud Computing systems do not require much interaction from the consumer's end since its software upgrade and maintenance are done systematically and remotely by the service providers. Also, Its high demand brings many unwanted security attacks. The most common attacks are Denial of Service (DoS), Cloud Malware Injection, Side Channel, Phishing, and VM Rollback. Both the service providers and users are at risk as all kinds of data are leaked when an attacker gains access to a cloud server. Leakages of credential information, private data, and unauthorized access to cloud resources are the usual results. It is critically important for Information Technology experts to tackle the unresolved security threats now before it is too late and affects major services.

Minhajul - Objectives

The objective for our research paper is to go over unresolved threats in cloud computing. Although there are many great benefits of cloud computing, there are also security threats and vulnerability. The following research paper will go over the concept of cloud computing, explore security and privacy issues, and provide solutions for them. We will also go over cost management and lack of resources in cloud computing.

Awais - Method

Data was collected for this problem through the resources found in the City Tech Library Database. We conducted our own research to find resources that help alleviate this project and make it a more resourceful project. We used terms such as 'Cloud computing, security threats in cloud computing, security issues in cloud computing, and unresolved threats in cloud computing.' There were multiple articles and books found that discuss the issues of security in cloud computing systems. The research looks efficient and most resources are relatively in range from 2015-2020 and updated and peer reviewed. The resources that we will be using throughout the project holds a lot of conducted studies from many journals. Most searches were in journals written by

Everyone - Results

As we did more research, we found that there are numerous cloud computing security and privacy issues. According to a Journal “Security and privacy issues in cloud computing” the five major attacks are Denial of Service (DoS), Cloud Malware Injection, Side Channel, Phishing, and VM Rollback. Also, traditional security attacks required many computers to generate a decent amount of computing power, but now Cloud computing technology is being used to execute security attacks due to its high computing power. To mitigate those security threats, information technology experts implement new security policies, access management, data protection, and advanced security techniques. (Journal of Defense Resources Management, 2014). Furthermore, a lot of the privacy issues can be resolved by having a well and trusted service agreement between the provider and the user.

Discussion

Ronald: The most common threats in Cloud computing are on the application level. Command and Malware injection attacks are currently the biggest security challenge across all deployment models of Cloud computing. Attackers create a new service application which is injected into cloud servers, the malicious application is designed to behave and be recognized as a genuine service of the servers. Once the injection is successful, user data is then redirected to the malicious application and attackers get access to all private data, credential information, and unauthorized cloud resources. According to a Journal "Exploring Security Issues and Solutions in Cloud Computing Services - A Survey" one of the major security threats are under protected APIs (Application Programming Interface), APIs are used by users in order to fully manage and control their cloud services. Weak and insecure API leads to exposure of private data and also makes it easier for attackers to inject malicious softwares. The journal provides five solutions to underprotected APIs. First, make sure that there's a secured communication between the APIs and clients. Second, APIs and all credentials, keys and tokens must have a strong authentication scheme. Third, design a stronger and more secured parser configuration of data. Fourth, have an active access control scheme that prevents attackers from getting access to unauthorized functions and data. Finally, prioritize protection for all injection attacks (Kumar, P Ravi, Raj, P. Herbert, Jelciana, P, 2017, pp. 13). The journal is a crucial source of information as it is peer reviewed and its publisher De Gruyter is an international academic publisher that is known to have published excellent written works for more than 270 years. Furthermore, according to a journal "Security and privacy issues in cloud computing" there are more possible ways to avoid injection attacks. The two main solutions are Security Policy Enhancement and Access Management. Security Policy Enhancement will apply new policies which will make it harder for attackers to get access to powerful cloud computing services as attackers usually launch their attacks with the use of cloud services. They would only need a valid credit card to start their malicious activities. So as a solution, information technology experts would need to set up stronger registration systems, credit card fraud monitoring and more public blacklists. Access Management proposes the idea that there should be active access control mechanisms that would monitor all the types of traffic in cloud computing. The traditional protocol only consists of monitoring private data which are stored in the cloud's physical computer storage. More firewalls and intrusion detection systems must be used to monitor all incoming and outgoing traffic online. The article recommends using authentication standards such as Security Assertion Markup Language (SAML) and extensible Access Control Markup Language (XACML). Both can be used to control access to cloud data and applications. Additionally, SAML will be used for monitoring the transfers of authentication between servers while XACML will be for establishing authorization. Both journals focus on the fact that prevention is key and that there

must be a well-established trust between the providers and users for cloud service providers to implement stronger security policies.

Minhajul: Cloud computing offers customers a more flexible way to obtain computation and storage resources on-demand, customers able to go to companies like Amazon and rent computing power and storage resources extremely cheap. Cloud computing has become more accessible within the past few years, however, it came with a drawback, which is security and privacy. The user data can be accessed by the host company with or without permission. The service provider may access the data that is on the cloud at any point in time. While doing research, I also found that in the process of trying to save money, time, and resources, these cloud computers may not do the necessary computations which could leave a back door to the server, leading to losing the clients' data. 0

A ,./wais: ;;0There are data security risks and issues in IT. Security and privacy are the two main concerns in cloud computing to protect the data. Security and data privacy issues can occur due to data breaching. Data breaching is unauthorized and no permission granted to access personal information. Data breaches require legal action to be taken. Hijackers can hack information and steal information and launch other attacks on the cloud. To prevent data from hackers extracting and deleting data, there should be multiple ways to protect the data. There is a technique to adding layers of security to your cloud. Having multiple layers of security prevents and creates a blockage for unauthorized users to go in and hack clouds with personal data. "A three-layered data security technique is proposed [34]: the first layer is used for authenticity of the cloud user either by one factor or by two factor authentications; the second layer encrypts the user's data for ensuring protection and privacy; and the third layer does fast recovery of data through a speedy decryption process (Zhang, 6)." Having multiple layers of protection and barriers prevents hackers from stealing information and leaking data from clouds.

Conclusions

Ronald: All in all, We've discovered that unresolved security threats in Cloud computing is a very broad topic. There are many emerging security and privacy threats. Additionally, the most common issues are on the application level. Attackers usually gain access to cloud servers through applications. As I researched solutions to application security issues, many of the solutions indicate that security threats exist due to the weak and insecure designs of applications. E.g. using software modules, frameworks, and libraries that are known to have vulnerabilities. (Kumar, P Ravi, Raj, P. Herbert, Jelciana, P, 2017, pp. 13). Many of the emerging security threats on the application level can be solved simply by making sure that the structure and communication of applications are always secured. Not only that, but also keep the libraries, frameworks, software modules, and operating systems always up to date.

Minhajul: Our conclusion regarding my discoveries is that cloud computing is a flexible way to obtain computation and storage resources on-demand. However, there's always risk of losing your data security and privacy. Since everything is online, there's no way to completely secure a server, there's always going to be a chance of you getting hacked. You can, however, implement some safety measures which can potentially help with lowering the chances of your data being breached. There are multiple issues that can be found regarding cloud computing, most of which could be prevented if cloud service providers start implementing the best security and privacy system when storing data on the cloud.

Awais: What we can conclude from all the results and discussions is that security and privacy threats in cloud computing can be dangerous in many ways. Researchers have attained a high level of data and security protection in cloud computing. Building layers of protection and barriers to your cloud whether sharing data or giving access to others to the data storage helps the cloud computing from staying confidential. As discussed, security and privacy are the biggest concerns and/or issues in cloud computing that need attention in IT. Researchers in IT are still evaluating more solutions that can lock and store data securely and safely. Cloud computing occurs in all organizations around the globe, and many types of data are stored in the cloud, so it is better to keep it private and lock it and prevent it from leaking any data out which causes conflicts. Further developed strategies and solutions are to be evaluated because not only one way will secure the data.

Recommendations

Ronald: I think that Cloud service providers must first establish a new service agreement with the users. A service agreement which will discuss boundaries between privacy and security since other solutions to security threats in Cloud computing involves traffic monitoring of all data. Moreover, information technology experts must be proactive in keeping their services up to date. They must also implement new access management and policies which will provide administrators the freedom to monitor more of the cloud. However, this must be done without invading the privacy of the users. According to a Journal "Security and privacy issues in cloud computing" it is hard for Cloud service providers to detect potential security threats since cloud computing laws prevent them from looking at user activities, so attackers are free to try and upload their malicious softwares to get access. Detection of malicious activities are mostly from security softwares which are running actively in the background (Journal of Defense Resources Management, 2014). Special boundaries must be set between users and service providers in order to design and utilize a new security prevention system.

Minhajul: There are multiple fixes for such issues, one of which can be used to make sure that the service provider has the best security is to use third-party auditors that have expertise and capabilities to do more efficient work and convince both cloud service providers and owners. Double-checking the data provided by the company about the security of the cloud will confirm if there's no way to get hacked. Data breaches is another issue which can be prevented by implementing timeout functions and stick to a strict security update procedure. Since attackers can access the server through an application, the users need to be mindful of what they download and install on the server. Which means if a big company is using a server, they need to educate their employees on data security. However, to be completely safe regardless of an attack or not, you may even decide to store data in-house as well as remotely for a hybrid cloud if your data is highly critical.

Awais: Since data security has been a major around the globe in information technology not only cloud computing, it is important to always have a strategy when saving the data anywhere. For data stored in the cloud to be protected, the data should be stored across multiple zones in the cloud, daily data backup is required and off-site storage is used for protection for keeping the data safe. Hybrid Technique is one solution that can be used to prevent data breach in cloud computing from occurring and causing threats or attacks through hackers because it is a technique that ensures data confidentiality. Multiple cloud databases in one cloud can be good to store confidential data so access is not easy and the data is divided. Also, if deleting the data from the cloud it is good to always encrypt the data and then delete it permanently.

References

Journal of Defense Resources Management. (October 2014). Security and privacy issues in cloud computing. https://advance-lexis-com.citytech.ezproxy.cuny.edu/api/document?collection=news&id=urn:contentItem:5FD7-0BS1-DYV1-93VF-00000-00&context=1516831.

Kumar, R. (2017). Exploring Security Issues and Solutions in Cloud Computing Services – A Survey. Cybernetics and Information Technologies : CIT, 17(4), 3–31. https://doi.org/10.1515/cait-2017-0039

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1155/2014/190903

Word Count: 2404