In Defense of Cloud Computing: A Summary

Soo Lim[1] and Taeyoon Kim[#]

[1]Yongsan International School of Seoul, Republic of Korea
[#]Advisor

ABSTRACT

With the advancement of cloud computing, it became possible to effortlessly host data storage and retrieve it without being hampered by physical limitations. However, the hosting of such an astronomical amount of data, and the ease with which the said data is retrieved, brought in unwanted security risks and crucial information links. A multitude of breaching methods, including Distributed Denial of Service (DDos), Man in the Middle (MiTM), Phishing, Zombie Attacks, and Side-Channel Attacks, have forced computer security engineers to address each individual issue lest critical information is stolen or misused. This paper will introduce the concept of cloud computing, the advantages it brings to data storage and management, and the disadvantages and weaknesses which are inherent to this technology. Additionally, this paper will analyze the intruding mechanisms of the five previously mentioned cloud security attack methods and then subsequently introduce the security protocols utilized by either business or individual research groups to remedy the issue.

Introduction

Cloud computing and storage have become major drivers of economic success for many companies over the past couple of years (Anouncia & Wiil, 2019). As an online platform that remotely takes in data in order to perform specified operations on big data, many companies and their respective cloud service providers offer their service as a software to allow customers to approach and process data effortlessly. Companies such as Twitter, Netflix, and Paypal utilize these platforms to control risk management, analyze live market data, manage their supply chains, and considerably more (Synenka, 2021). Other tech giants such as Google and Microsoft are continuously adding infrastructure to their already vast cloud ecosystem (M. Zhou et al., 2010). As applications of cloud computing are fueled by big data, companies employ cloud computing to implement the potential of the immense quantities of data for their benefit. In order for companies to realistically obtain financial gains, there are necessary advantages that cloud computing must bring to these companies. Cloud computing does this effectively with a combination of multiple assets.

With limitless resources in these services, it allows the user or company to pay accordingly for the resources that were actually used, allowing for scalability. This thus naturally leads to a reduction in costs through a decrease in unnecessary resources; by having access to these platforms through software, it allows companies to diminish costs for enormous capital expenses such as data centers. And as cloud computing has flexibility, many resources and services are deployed in most global regions. Due to this, many data and processing activities can be directed to take place proximally where the task is located.

Cloud computing, however, also comes with disadvantages that are undeniably crucial for its users. Some of the biggest negatives of cloud computing are security breaches. To assess some of its impacts, threats, and what it breaches, the STRIDE method will be used as somewhat of an objective indicator of the damage (Khan et al. 2017). “These include, but are not limited to, misappropriation of confidential information, uncontrollable use of cloud services, data propagation, potential unauthorised secondary usage, trans-border flow of data, and dynamic provisioning” (Abdulsalam & Hedabou, 2021). In an attempt to combat these threats, measures have been taken to prevent damage at personal, software, and institutional levels.

Many people have been educated on identifying potential frauds, such as not clicking on malicious links, while on a software level, programmers constantly update security patterns to fill in the holes of their system. Additionally, institutions have implemented new user identification models to counter malicious attacks.

Companies such as Apple include the "Secure Enclave", which is a dedicated AES cryptographic engine, in their processors to ensure an extra layer of security (Apple, 2022). Google ensures security through two factor authentication of users' emails, and also by recording the login device, location, and time and transmitting this information to the user (Rankin, 2017; Google, 2022). This allows the user to monitor their own activity and identify when a security breach has occurred in their account. Through these security measures, users are able to secure their privacy via changing their password. Additionally, even if their password has been leaked, as long as the two factor authentication system is set in place for the user, there is very little chance of the users getting breached. The two factor authentication system requires the user to go onto a device they are already logged in with on their account, and confirm whether they were actively trying to login.

Major Security Threats

The ease of which cloud computing is under constant threat is a natural consequence of interface and protocol. Tightening security measures and building a virtual fence to keep the invaders out will only lead to cloud computing being a virtual infrastructure that exists in the ethernet of a company or facility. This goes against the very purpose of cloud computing. As a result, security regarding cloud computing has to have an amorphous defense mechanism which can change depending on the threat perceived

DDoS

One prominent attack against security protocols is Distributed Denial of Service (DDoS). A DDoS attack is when the attackers intend to induce immense traffic onto a website to overwhelm it (Wu et al., 2011). What is distinctive about this attack is that it does not actually breach any security perimeters. Rather, the attack intends to make the target website nonfunctional to its users. Thus, the bigger the userbase is for the website, the bigger its ramifications will be, especially when the impact of this attack lasts for weeks, or even months. These ramifications may include loss of revenue, theft of data, compensation to business partners, and even reputational damage.

DDoS is difficult to counter because the attack comes from multiple connected devices. These connected devices are called botnets, which are defined as "large clusters of connected devices infected with malware that allows remote control by an attacker," hence the attack name, Distributed Denial of Service (Imperva, 2020). This allows for the traffic to be distributed amongst many devices, making it difficult for security tools to detect it as an attack.

To combat these problems, Google devised a solution based off CAPTCHA in order to create reCAPTCHA (Google, 2022). Google claims that reCAPTCHA uses "an advanced risk analysis engine and adaptive CAPTCHAs to keep automated software from engaging in abusive activities" ("Google"). reCAPTCHA has many forms of questions for the users, including selecting images with certain objects in them, identifying warped words, or listening to audio and determining the word or number being said. These procedures only allow legitimate users to pass this "security checkpoint", it can successfully prevent attackers from overloading the website.

Another option many companies utilize is employing other businesses that expertise in DDoS protection. Some options include Arbor Networks Sightline, Flowspec, Juniper Networks & Corero, F5 Silverline Web Application Firewall, and many more (Nomios Group, 2021). Considering the impacts a DDoS attack may bring to any company, a DDoS protection must be set in place. Rather than diminish customer experience, reputation, and financial value, it would be wise to invest sufficient money into DDoS protection to prevent the attack in the first place; a preventive medicine strategy for cloud security (National Cyber Security Centre, 2020).

Man in the Middle

If DDoS attacks are focused on causing pressure on the server itself, the Man in The Middle (MiTM) attempts to intervene itself between two existing poles, the sender and the receiver. However, unlike eavesdropping on a tapped phone line, MiTM goes beyond and attempts to modify the original message while stealing its content for personal use, a process known as spoofing (Javeed & MohammedBadamasi, 2020). Although there are a plethora of attack routes utilized by MiTM attackers, this article will focus ARP Spoofing and DNS Spoofing.

ARP Spoofing

ARP spoofing is short for address determination protocol. ARP spoofing abuses the ARP protocol, as the protocol was not designed for security. The ARP protocol is executed when the host cannot identify the MAC (Media Access Control) address of the specified IP address. By not actively inspecting whether the request comes from an authorized party, the attacker can easily intercept communication between the two parties (Herzberg & Shulman, 2012; Imperva, 2020).

A prominent use of ARP spoofing by attackers is dynamic eavesdropping. As the attacker is able to intercept the communication, they can abuse this attack to modify their messages in order to diminish trust, record their messages to cause reputational damage, or break business deals between the two parties. The bigger the reputation/fame of the two parties, the more consequential damage ARP spoofing may produce. ARP spoofing is a major threat that many companies need to address through security programs and protocols. This article will examine the multiple ways that ARP spoofing can be detected and solutions companies have devised to counter this security threat. Some effective detection methods are cryptographic, voting-based, server-based, and host-based.

The first method utilizes a cryptographic environment which "depends on civic basic cryptography for ARP response verification" (Sun et al., 2009). This allows for the verification of an ARP response, and as a result also forces an authenticating regarding the validity of the user. Naturally, when the validity of the user is checked and identified to be "true", ARP spoofing can be prevented. Another mechanism to acknowledge the ARP response is the voting-based solution. In the voting-based solution, whenever there is an ARP response, the MITM-Resistant Address Resolution Protocol MR-ARP will inquire the device and "authenticate whether the device practices the novel IP address" (Javeed & MohammedBadamasi, 2020).

The server-based solution treats the situation in two-fold ways (Salim et al., 2012). In the first situation, the Server Handler focuses on identifying the Received ARP Packets (SHRP) to verify the presence of a natural MAC. If the MAC is deemed to be "false" the SHRP will utilize an algorithm to analyze the incoming data. Additionally, in the second situation, the Server Handler focuses on the Control Message (SH_CM). This method focuses on the control messages implanted within ARP packets. If the control messages inside the packets are deemed to be of suspicious nature, it will use the same process as SHRP and an algorithm will be used to clarify the contents of the package. In the host-based solution is when there exists a middleware, the software between the operating system and applications on the system, which asynchronously recognizes and deters ARP spoofing (Microsoft, 2022; Bai et al., 2011).

DNS Spoofing

Unlike ARP spoofing, DNS spoofing is inherent in the domain of the website itself, controlling the DNS access from the target in order to redirect them to a rogue server; the text itself is susceptible to being attacked directly (Hussain et al., 2016; Imperva, 2019). DNS spoofing is straightforward to detect with a method called an "entropy increasing mechanism". This mechanism cannot ensure defense against DNS spoofing, but does decrease its influence. The extra entropy adds an extra unpredictability to DNS packets for intertwining the inoculation to the false DNS responses (Ludena Romana & Musashi, 2007).

Another method by which DNS Spoofing can be prevented is by coding the otherwise plain text so the information is impossible for the hacker to understand. A cyber cipher will encrypt the response name server IP and query ID to prevent the hacker from gaining access or even guessing the location of the site (Hussain et al., 2016).

Phishing

Different from DDoS attacks or MiTM attacks, phishing has the main purpose of stealing the target's personal information. Phishers will attempt to swindle users by sending out fraudulent messages in order to obtain their personal identity. Oftentimes, the link that is sent to the intended target will redirect them to the attacker's replicate website. The website will ask for the user's username, password, credit card details, social security number, etc. This will aid the attacker in identity theft, allowing them to use the victim's information freely. There are many types of ways the attackers can deceive the victims. This may include code-based key-loggers, search engine phishing, mass e-mailing, and etc. (Purkait, 2012). Countermeasures against phishing include, but are not restricted to, stopping phishing at the e-mail level, security and password management toolbars, anti-phishing training, and continual OS updates (Purkait, 2012).

As mass distributing e-mails for bank account details, for example, costs almost next to nothing, it was, and still is, a common way of phishing. One solution that has been proposed to counter this type of attack is to create a specialized, machine-learning filter. Utilizing a filter named PILFER, proved that constantly adapting machine-learning filters may prove to be an useful autonomous defense system capable of combating phishing (Fette et al., 2006). In a different method found by Segal et al. (2004), they utilized a combination of multiple disparate classifiers, labeled Spamguru, and were found to detect spam at very low false positive rates. The solutions mentioned above come with limitations that specifically pertain to the matter of phishing, however. Employing spam filters can encourage phishers to merely hide key words and flags in their e-mails to avoid these filters. Active use of spam filters also may classify certain e-mails that are legitimate into the spam category. The biggest downfall of the spam filters may be the fact that it will make users overconfide in the spam filters, endorsing the thought that everything that comes in their inbox is a legitimate e-mail.

Having security and password management toolbars effectively means that the user employs software or extensions in their respective OS or browser in order to avoid phishing. A tool Jendricke and Markotten (2000) have proposed is a "identity manager", a means by which the user can configure the security features in order to protect them against malicious internet applications (Jendricke & Markotten, D. 2000). For a tool that comes in the form of an extension, Halderman et al., (2005), proposed a solution in which the extension allows the user to remember one master password. The extension would use "strengthened cryptographic hash function to compute secure passwords for arbitrarily many accounts", which would in effect, allow the user to have only memorized one password while creating safe passwords that would provide the most protection from spoofing.

Anti-phishing training is not a program or a software that actively prevents the user from getting phished, but rather educating the users to protect themselves. Sheng et al. (2007) conducted an experiment with an educational game, and found that the game reduced a user's tendency to click on phishing webpages around equal, if not better than reading training material on phishing by eBay's, Microsoft's Security Tutorial on Phishing, the Phishing E-card from the U.S. Federal Trade Comission, and a URL tutorial from MySecureCyberSpace portal (Sheng et al. 2007). This shows the potential for the mass distribution of effective anti-phishing training through a game accessible to everyone.

OS services such as Windows and Macintosh have built in security services that help prevent users from getting attacked by phishers. They are enabled by default and are an official security system created by these companies. As new phishing methods appear, new updates are distributed to users in order to protect them from new attacks. Along with new updates, users must be reminded to update their OS to get the most up-to-date defense on their device.

Zombie Attack

A zombie attack is one of the more sophisticated attacks, as a single breach or contamination will lead to a chain reaction (Cloud computing news, 2013). While in the past zombie computers were physical manifestations of compromised hardware, zombie attacks in cloud computing result from an infestation from a virtual machine (Kumar & Singh, 2017). The mechanism by which a zombie attack happens to a cloud server is relatively straightforward. A forgotten or neglected system or node is left without the latest security upgrades (Siemons, 2017). Such systems may be suspect to state of the art virus attacks, and this may become infected. This allows the intruder who introduced the virus to use this system as a forward base to attack other nodes within the system.

A constant monitoring of deficient systems is the best solution to solving Zombie Attacks, but in the case where human error neglects to eliminate an unused system, a method by which the cloud system itself identifies and isolates a contaminated system is the second best answer. Agbedemnab et al, (2020) suggested using a strong authentication method by making the virtual machine (VM), a node between a legitimate user and cloud service provider, the gatekeeper of all incoming data. The research team used "The asymmetric cryptography for authentication and XOR decipher for encrypting the user public key during login" to sufficiently authenticate incoming messages and data from the user side. If the data being sent from the user side was legitimate, it was granted further access towards the cloud service provider. If the data was deemed to be "false" it was blocked.

Side-Channel Attacks

Side-channel attacks don't directly target the code, but rather exploits information on how the program works. What this essentially means is that the attacker attempts to observe the direct and indirect effects of the program, and exfilitrate sensitive information (Wright, 2021). Side-channel attacks have become more common because of more sensitive measuring tools. These tools allow attackers to "gather extremely detailed data about a system while it is running" (Wright, 2021). Additionally, side-channel attacks are difficult to defend against, as they leave very little to no trace and do not directly alter any systems. Thus, special security protocols must be utilized to defend against side-channel attacks. Presented by Zhang et al., (2016) their CloudRadar system detects side-channel attacks and also "requires no changes to the hardware, hypervisor and guest VM and applications". Alongside this system, the user can make apt decisions and changes to alter their program to effectively secure their program. General defenses proposed in previous studies to side-channel attacks are partitioning caches, randomization, and avoiding co-location.

DNS Spoofing

Unlike ARP spoofing, DNS spoofing is inherent in the domain of the website itself, controlling the DNS access from the target in order to redirect them to a rogue server; the text itself is susceptible to being attacked directly (Hussain et al., 2016; Imperva, 2019). DNS spoofing is straightforward to detect with a method called an "entropy increasing mechanism". This mechanism cannot ensure defense against DNS spoofing, but does decrease its influence. The extra entropy adds an extra unpredictability to DNS packets for intertwining the inoculation to the false DNS responses (Ludena Romana & Musashi, 2007).

Partitioning Caches

This is one of the most straightforward ways that has been found to defend against side-channel attacks. By preventing "cache sharing by dividing the cache into different zones by sers or ways for different VMs" (Zhang et al., 2016). This defense method can be achieved through hardware or software means.

Randomization

Unlike ARP spoofing, DNS spoofing is inherent in the domain of the website itself, controlling the DNS access from the target in order to redirect them to a rogue server; the text itself is susceptible to being attacked directly (Hussain et al., 2016; Imperva, 2019). DNS spoofing is straightforward to detect with a method called an "entropy increasing mechanism". This mechanism cannot ensure defense against DNS spoofing, but does decrease its influence. The extra entropy adds an extra unpredictability to DNS packets for intertwining the inoculation to the false DNS responses (Ludena Romana & Musashi, 2007).

Avoiding Co-location

This method focuses more on VM in order to reduce the co-location possibility between the victim and the attacker VM. The way Zhang et al. (2016) and tested this was through migrating VMs to increase the difficulty of VM co-location for the attackers.

Discussion

Cloud computing has helped ease the way companies and individuals store and process crucial information. The online nature of the data processing always gives any user easy access as long as there is a stable internet connection, but it is also this very nature that makes cloud computing vulnerable to malicious users. For individual users it may result in the loss of personnel information such as user name, password, bank account numbers, social security numbers, and consequent malign usage of said information for unwanted monetary transactions. (Webroot, 2022). For businesses and institutions, a breach in their cyber defenses results in the theft of critical business information and clientele list. Additional repercussions of a cyber breach include inerasable damage loss to the business's reputation, and compromise of future prospects.

Ironically, the best defense against cyber attacks is the education of the personnel that use the system. The user and the maintenance operators have to know possible attack routes and make sure their software is up to date. Aside from the human error side of cloud security, the software defense uses defense protocols that are skilled at identifying false signs and non-benign authentication attempts. Proper identification of the user before their access to the cloud service provider, and the ability of the system to defend itself against continuously changing malware attacks, remain the backbone of a properly defended cloud system. An argument may be made that advanced algorithms may provide more sophisticated defense measures, but even those algorithms are at their core, a simple check the ID and password method; it is just how the algorithm checks the ID and password which is different.

Nevertheless, the responsibility regarding the protection of sensitive data is dependent on the cloud service providers themselves. There have been movements by these service providers to distance themselves from this responsibility, as they are seen to rely more upon third party institutions to guarantee the security of their cloud infrastructure (Abdulsalam & Hedabou, 2021). However, such proceedings will give way to situations where a robbery has taken place but nobody is responsible for the stolen gold, or in this case data. Up to date security protocols and significant training of the maintenance team has been and always will be the best line of defense in cyber security.

Acknowledgments

I would like to thank my advisor for the valuable insight provided to me on this topic.

References

Anouncia, S. M., & Wiil , U. K. (2019). *Knowledge computing and its Applications: Knowledge manipulation and*. SPRINGER Verlag, SINGAPOR.

Valentina Synenka, *Top 10 Companies Using Cloud and Why*. CustomerThink. (2021, August 31). Retrieved May 30, 2022, from https://customerthink.com/top-10-companies-using-cloud-and-why/

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. *2010 Sixth International Conference on Semantics, Knowledge and Grids*, 105-112.

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). Stride-based Threat Modeling for Cyber-physical systems. *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 26–29 September 2017; pp. 1–6.* https://doi.org/10.1109/isgteurope.2017.8260283

Abdulsalam, Y. S., & Hedabou, M. (2021). Security and Privacy in Cloud Computing: Technical Review. *Future Internet*, *14*(1), 11. https://doi.org/10.3390/fi14010011

Apple. *Introduction to apple platform security*. Apple Support (2022). Retrieved May 30, 2022, from https://support.apple.com/en-ie/guide/security/seccd5016d31/web

Rankin, K (2017, March 9). *Two Factors are Better than One*. Linux Journal. Retrieved May 30, 2022, from https://www.linuxjournal.com/content/two-factors-are-better-one

Google. (2022). *Best practices for a more secure login in google cloud.* Google. Retrieved May 30, 2022, from https://cloud.google.com/blog/products/identity-security/best-practices-for-a-more-secure-login-in-google-cloud

Google. *ReCAPTCHA*. Google (2022). Retrieved May 30, 2022, from https://www.google.com/recaptcha/about/

Wu, Z., Wang, C., & Zeng, H. (2011). Research on the comparison of flood DDoS and low-rate Ddos. *2011 International Conference on Multimedia Technology*. https://doi.org/10.1109/icmt.2011.6002141

Imperva. *What does ddos mean?: Distributed denial of service explained: Imperva*. Learning Center. (2020, September 30). Retrieved May 30, 2022, from https://www.imperva.com/learn/ddos/denial-of-service/

Nomios Group (2021, Jan 21). *Top 6 ddos protection solutions that should be on your Radar*. Nomios Group. Retrieved May 30, 2022, from https://www.nomios.com/news-blog/top-ddos-protection-solutions/

National Cyber Security Centre (2020, Dec 16). Measures to counter ddos attacks. National Cyber Security Centre. Retrieved May 30, 2022, from https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ddos.html

Javeed, D., & MohammedBadamasi, U. (2020). Man in the middle attacks: Analysis, motivation and prevention. *International Journal of Computer Networks and Communications Security*, *8*(7), 52–58. https://doi.org/10.47277/ijcncs/8(7)1

Herzberg, A., & Shulman, H. (2012). Antidotes for DNS poisoning by off-path adversaries. *2012 Seventh International Conference on Availability, Reliability and Security*. 2012, https://doi.org/10.1109/ares.2012.27

Sun, H.-M., Chang, W.-H., Chang, S.-Y., & Lin, Y.-H. (2009). DepenDNS: Dependable mechanism against DNS cache poisoning. Cryptology and Network Security, 174–188. https://doi.org/10.1007/978-3-642-10433-6_12

Bai, X., Hu, L., Song, Z., Chen, F., & Zhao, K. (2011). Defense against DNS man-in-the-middle spoofing. Web Information Systems and Mining, 312–319. https://doi.org/10.1007/978-3-642-23971-7_39

Salim, H., Li, Z., Tu, H., Guo, Z. (2012). A Client/Server Based Mechanism to Prevent ARP Spoofing Attacks. In: Tan, Y., Shi, Y., Ji, Z. (eds) Advances in Swarm Intelligence. ICSI 2012. *Lecture Notes in Computer Science*, vol 7332. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31020-1_30

Imperva. (2020, May 6). *What is ARP spoofing: Arp cache poisoning attack explained: Imperva*. Learning Center. Retrieved May 30, 2022, from https://www.imperva.com/learn/application-security/arp-spoofing/

Microsoft. (2022). *What is middleware - definition and examples: Microsoft Azure*. Microsoft Azure. Retrieved May 30, 2022, from https://azure.microsoft.com/en-us/overview/what-is-middleware/#:~:text=Middleware%20is%20software%20that%20lies,data%20management%20for%20distributed%20applications

Hussain, M. A., Jin, H., Hussien, Z. A., Abduljabbar, Z. A., Abbdal, S. H., & Ibrahim, A. (2016). DNS protection against spoofing and poisoning attacks. *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*. https://doi.org/10.1109/icisce.2016.279

Imperva. (2019, December 29). *What is DNS spoofing: Cache poisoning attack example: Imperva*. Learning Center. Retrieved May 30, 2022, from https://www.imperva.com/learn/application-security/dns-spoofing/

Ludena Romana, D., & Musashi, Y. (2007). Entropy Based Analysis of DNS Query Traffic in the Campus Network. Journal of Systemics, Cybernetics and Informatics. 6.

Fette, I., Sadeh, N., & Tomasic, A. (2006). Learning to detect phishing emails. https://doi.org/10.21236/ada456046

Segal, R.B., Crawford, J., Kephart, J., & Leiba, B. (2004). SpamGuru: An Enterprise Anti-Spam Filtering System. *CEAS*.

Halderman, J.A., Waters, B., & Felten, E.W. (2005). A convenient method for securely managing passwords. *WWW '05*.

Jendricke, U., & Markotten, D.G. (2000). Usability meets security - the Identity-Manager as your personal security assistant for the Internet. Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00), 344-353.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS '07*. https://doi.org/10.1145/1280680.1280692

IBM (2016, September 21). *Kill cloud zombies before it's too late*. Cloud computing news. Retrieved May 27, 2022, from https://www.ibm.com/blogs/cloud-computing/2013/05/31/cloud-zombies/

Kumar S., & Singh M. (2017) *Detection and Isolation of Zombie Attack under Cloud Environment*. Orient.J. Comp. Sci. and Technol;10(2) http://dx.doi.org/10.13005/ojcst/10.02.12

Siemons F., *Security Concerns Around Zombie Cloud Infrastructure* (2017). Retrieved May 30, 2022, from https://resources.infosecinstitute.com/topic/security-concerns-around-zombie-cloud-infrastructure/

Agbedemnab, P. A., Abdul-Mumin, S., & Abdulrahim, Z. (2020). Identifying and isolating zombie attack in cloud computing. *Asian Journal of Research in Computer Science*, 46–56. https://doi.org/10.9734/ajrcos/2020/v6i230157

Wright, G., & Gillis, A. S. *What is a side-channel attack?* SearchSecurity. (2021, April 6) Retrieved May 30, 2022, from https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=A%20side%2Dchannel%20attack%20is,program%20or%20its%20code%20directly.

Zhang, T., Zhang, Y., & Lee, R.B. (2016). CloudRadar: A Real-Time Side-Channel Attack Detection System in Clouds. *RAID*.

Webroot. *The dangers of hacking and what a Hacker*. Webroot. Retrieved May 29, 2022, from https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-hackers

Dhillon, G. (2015). *What to do Before and After a Cybersecurity Breach*. The Changing Faces of Cybersecurity Governance Series.

Abdulsalam, Y. S., & Hedabou, M. (2021). Decentralized Data Integrity Scheme for preserving privacy in cloud computing. *2021 International Conference on Security, Pattern Analysis, and Cybernetics （SPAC)*. https://doi.org/10.1109/spac53836.2021.9539946