**DDoS Attacks In Cloud Computing**

Maham Rasheda

CIS 3120 MUA

Maham Rasheda

Zicklin School of Business

[maham.rasheda@baruchmail.cuny.edu](mailto:maham.rasheda@baruchmail.cuny.edu)

**Abstract —** The development of Cloud Computing has taken businesses by storm. As it provides computer services like storage, virtual machines and other applications. Even with these on-demand services Cloud Computing still faces cyber attacks like DDoS Attacks. Therefore, this research paper aims to thoroughly define Cloud Computing and DDoS. Furthermore, the paper will provide the negative effects DDoS plays in Cloud Computing. The paper will also present possible DDoS protection and tools. Evidence will be gathered from data sources such as articles, reports, journals, business news, to further analyze Cloud Computing, DDoS and the future in cloud .

***Keywords:*** cloud computing, future, applications, effects

1. Introduction

Oftentimes people talk about Cloud Computing being the “next new thing”, creating a deception to others that this type of technology started recently. In reality Cloud computing has started since the 1960s. This technology has significantly developed over the years broadening their services to all different businesses. The Cloud enables different features and characteristics that help run services in a faster and more efficient way. However, there has been a rise in DDoS attacks in the cloud that has negatively affected cloud computing. Given that there are DDoS attacks in the Cloud, there are also possible mitigation measures in place. This paper will present a comprehensive discussion on Cloud Computing, DDoS Attacks and Solutions.

1. General background

There’s quite a bit of a historical timeline within the Cloud Computing area. Cloud computing concepts were first introduced by John McCarthy in the 1960s. 10 years down the line the program of Virtual Machines or VM was born[1]. In 1990, companies started to offer virtualized private network connections. In 2006, Amazon Web Services was created by Amazon. It was the first company to advertise cloud computing to the public. At this point the public wasn’t as aware as to what Cloud Computing was. It wasn't till 2007 where Cloud Computing started to become more popular. Companies started to realize that Cloud computing is needed in order to store, protect, access their information systems all under one service. Then a year later, there was a discussion of if there should be more cloud computing services built. In that same year Microsoft launched Microsoft Azure; a cloud computing server to help with management systems. In addition, Oracle cloud was released in 2016 that provides storage,network, and applications over the internet. The question is what exactly is Cloud computing and what does it look like?

1. Cloud Computing

Cloud computing is the ability to provide cloud services over the internet. Cloud computing offers services such as storage, servers, databases, networking, software, access, analytics, intelligence and security [2]. In these servers it gives organizations the ability to have complete control over their cloud servers and security. When businesses invest in Cloud computing it helps them keep up with market demands. Additionally, there are three different types of cloud computing that have different requirements. Public cloud is a model computing that has services accessible to the whole business. Customers don’t have access to this type of cloud, and can’t customize it to their liking. Private cloud is hosted by one business, it’s known to have the most security. Lastly, there’s hybrid cloud which includes public and private cloud together. This cloud allows both consumers and businesses to interact smoothly. With different types of cloud computing there’s also different layers to the cloud.

1. Layers of Cloud Computing

Cloud computing has three service layers: Infrastructure as a Service(IaaS), Platform as a Service(PaaS), Software as a Service(SaaS). Infrastructure as a Service is a type of service that gives users the ability to store, compute and network resources whenever they need(Watts). Examples of IaaS are: Azure, Ibm cloud, Oracle, AWS. Platform as a Service is where companies provide resource tools to those who need it over the internet. Examples of PaaS are GoogleApp engine, Heroku. PaaS has flexibility meaning it’s available through public, private, and hybrid clouds as well. Software as a Service lets the cloud provider manage every application like virtual machine, data storage, servers, network. Examples of SaaS are dropbox, google apps, office 365 and slack. This platform is also very accessible. These three layers are one of the reasons why cloud computing is useful.

1. Cloud Security Uses

As mentioned, Cloud computing provides applications and infrastructure that is useful for many reasons. The way cloud computing is set up makes it financially feasible for businesses to employ it. It enables cost savings in computing and IT [2]. In addition, companies and users can choose how to pay for cloud services, giving them flexibility. Collaboration between business personnel and clients is another useful service offered by cloud computing. Businesses are confident that all information will be securely and safely backed up as they offer their staff cloud-based solutions for collaboration. The cloud does offer data backup, which enables loss prevention. Additionally, there are extra security precautions in the cloud, where hosts can specify application security settings and monitor data. In contrast to physical IT services, there is no practical means to retrieve someone's data in the event of a disaster. However, cloud services enable disaster recovery, which means they can reclaim data in the event of any catastrophe, no matter how big or small.Even with all of the advantageous features of the cloud, it is still not particularly secure from DDoS attacks.

1. DDoS Attacks

Distributed Denial of Service, or DDoS, is a category of network assault. Attackers carry out this attack by flooding the server with traffic from numerous websites. These web servers are only capable of handling so many queries at once. Therefore, the website will soon slow down and eventually fail when the server is overwhelmed by incorrect requests. Leading users to be unable to effectively use the online service. DDoS assaults may endure for several days, weeks, or even months. It may even consist of several attacks spaced out over time or simply one attack. Attackers frequently target large corporations or government websites in order to spread their message. It causes data loss, financial data loss, and credibility loss.

1. DDoS attacks in Cloud Computing

DDoS attacks still occur in the cloud, despite the fact that cloud computing is thought to be a better option for data protection. First, the attackers establish a reason to attack. The cloud environment hosts virtual machines that most of the time requires the internet to function. With that being said, the attackers identify the network and familiarize themselves with it. Then, they look for network vulnerabilities or places where there is insufficient protection. After that, they overwhelm the company's network with pointless data, causing system traffic. If a DDoS attack on a user's internet connection causes damage, that damage will then spread to cloud-based virtual servers [3]. As a result, the performance of cloud services suffers. One of the main goals of DDoS attackers is to make sure that the virtualization of the business doesn't work and that users can't access cloud resources. Lack of access may negatively affect employees and may result in data loss, messed-up storage, low availability and improperly configured security configurations. DDoS attacks are classified into three types, each of which includes a variety of attacks.

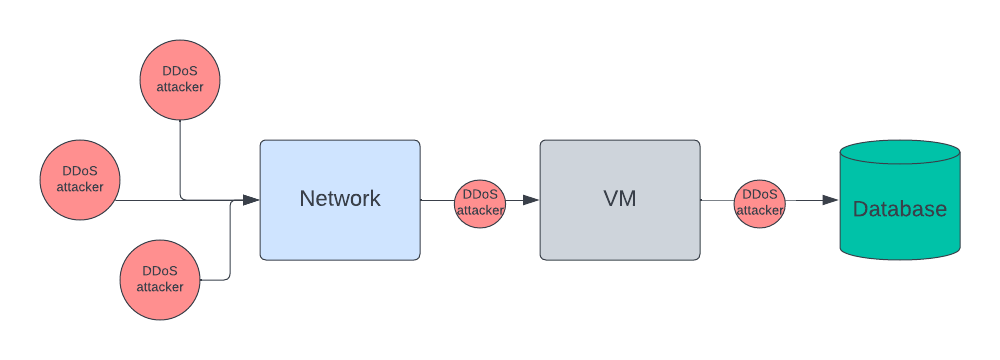


Figure 1: Explains the Process of DDoS attacks in Cloud especially without firewalls

1. Classification and types of DDoS attacks

DDoS attacks can be put into groups based on their level, such as application or network. At the network level, TCP, UDP, and ICMP are used in DDoS attacks. There are also volume attacks, protocol attacks, and amplification attacks, which are all different types of attacks. In a volume attack, the attacker sends multiple packets to try to use up all of the target server's resources before overloading the system and making it inaccessible[4]. Traffic attacks are another name for volume attacks. Then, in protocol attacks, the attacker gets around defenses by using flaws and exploits in the protocols themselves, such as the TCP SYN flood, TCP SYN-ACK flood, etc. An amplification attack is when an attacker sends a lot of packets to an IP address. This slows down the router. Flood attacks are also a type of protocol and amplification attack. They happen quickly because zombies clog up the network of the victim. Last but not least, application-level attacks try to overwhelm the servers and take over all the resources that consumers use. Reports say that a lot of DDoS attacks fit into this group[5].

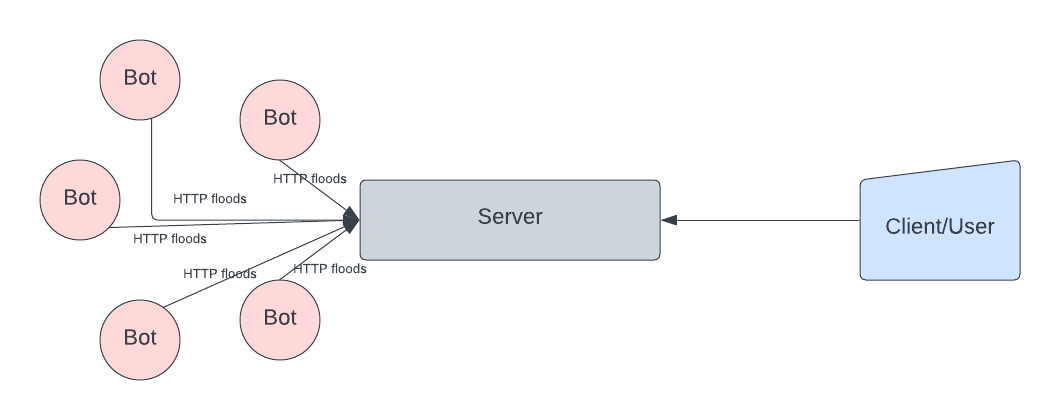
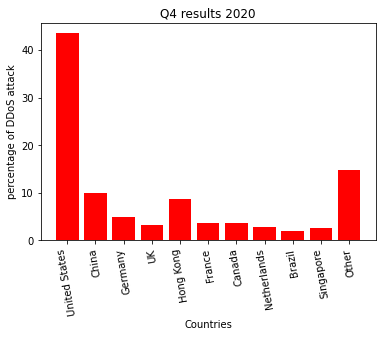
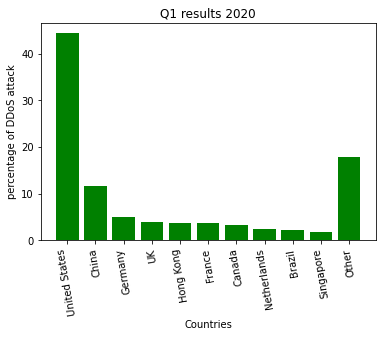


Figure 2: A diagram of HTTP Flood Attack which is categorized in a Application Level

1. Statistics of DDoS attacks in the Cloud

It’s important to understand the severity of these attacks in the Cloud. Due to how serious it has been reported that there’s about one-third of reported DDoS attacks on cloud services[6]. This indicates that attacks are occurring on the cloud and are evident. It’s been reported that the pay-as-you-go service in the cloud models have been exploited the most.Cloud computing is a service that is provided and used from countries all around the world. Due to how serious DDoS attacks are, more than 20% of businesses worldwide had at least one reported DDoS attack event on their infrastructure [6]. DDoS attacks on the cloud have become a much rather global issue. The figures below show charts of quarterly reports of DDoS attacks from countries like the USA, UK, Brazil, China etc. It’s quite evident that the United States faced the most DDoS attack . In Q1 they had about 44.34% more attacks than compared to Q4 where they had 43.55% . The country that had the least number of attacks was Singapore, attacks coming in up to 5% below in both quarters[7]. A DDoS assault can cause financial losses of up to 444,000 USD, no matter how small or large the strikes are on any nation [6]. It’s important to look at how to combat the solutions.

Figure 3: Q1 data results Figure 4: Q4 data results



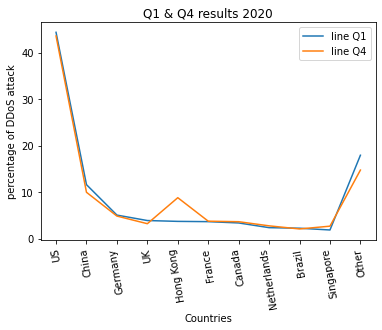


Figure 5: Comparative Trendline between Q1 & Q4

1. Cloud Based DDoS Protection

DDoS attacks against clouds are happening more and more often, so it's important to have the right protections in place. A detection method is one of the things that can be done. At first, the system stops or drops any attacks that look like they might be coming before they get to the server. After the attack has been stopped, the next step is to find out who did it [9]. Their IP address or ICMP traceback can be used to find them. Attacks can also be kept out of the game. This method makes sure that only good traffic gets into the system [10]. Ingress/egress filtering and Route-based packet filtering are two well-known ways to filter. Ingress filtering stops people from lying about their IP address. Malicious traffic that is leaving a local network is stopped by egress filtering [10]. Advanced ingress filtering is route-based packet filtering. It traces the route information and finds out more about where the address came from. Another great way to stop DDoS attacks is with the honeypot mechanism. Its goal is to get attackers by looking like a network to trick them. So, if an attacker tries to attack but fails, the Honeypot system can record the attack and find out who did it. So, businesses can not only keep their data safe, but also find out more about the person who attacked them.

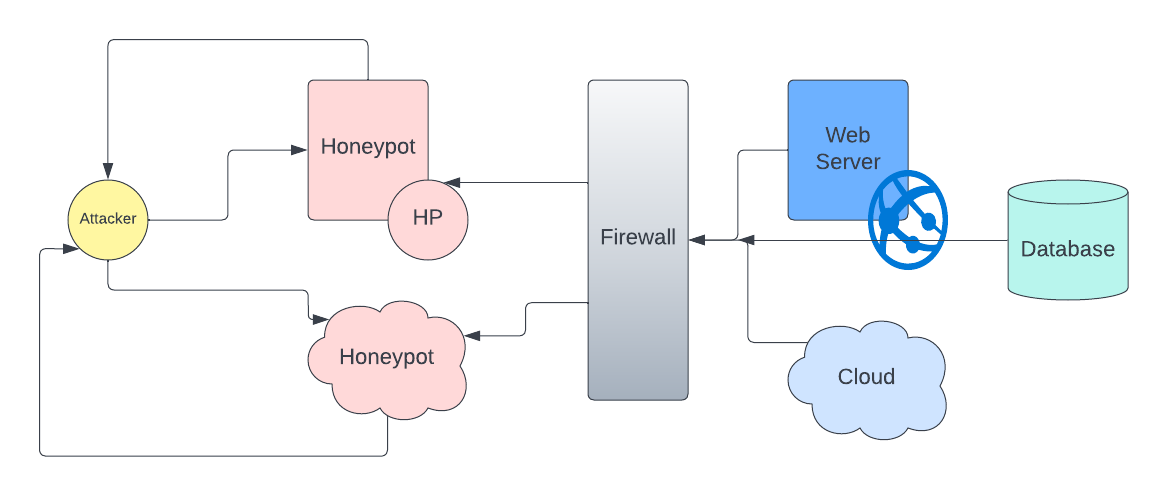


Figure 6: Diagram of honeypot process

1. Conclusion

Cloud computing no doubt is one of the most groundbreaking and on demand computer systems to be created. This paper thoroughly analyzed what cloud computing is, the different cloud models, and layers. Cloud computing provides flexibility and efficiency to businesses all across the world. The cloud computing system is not perfect, just like any other system. To conclude, businesses must realize that cloud security needs to be addressed because it is inadequate given the rise in DDoS attacks, particularly in the US.

References:

[1] “A brief history of cloud computing,” *Cloud computing news*, Aug. 23, 2016.<https://www.ibm.com/blogs/cloud-computing/2016/08/23/a-brief-history-of-cloud-computing-2/>

[2]P. K. Paul and M. K. Ghose, “Cloud Computing: Possibilities, Challenges and Opportunities with Special Reference to its Emerging Need in the Academic and Working Area of Information Science,” *Procedia Engineering*, vol. 38, pp. 2222–2227, 2012, doi: 10.1016/j.proeng.2012.06.267

[3]R. V. Deshmukh and K. K. Devadkar, “Understanding DDoS Attack & its Effect in Cloud Environment,” *Procedia Computer Science*, vol. 49, pp. 202–210, 2015, doi: 10.1016/j.procs.2015.04.

[4]S. Ison, L. Budd, M. S. Mahmoud, and Y. Xia, Eds., “Chapter 3 - Distributed denial-of-service attacks,” *ScienceDirect*, Jan. 01, 2020. https://www.sciencedirect.com/science/article/pii/B9780128187012000111

[5]O. Bamasag, A. Alsaeedi, A. Munshi, D. Alghazzawi, S. Alshehri, and A. Jamjoom, “Real-time DDoS flood attack monitoring and detection (RT-AMD) model for cloud computing,” *PeerJ Computer Science*, vol. 7, p. e814, Jun. 2022, doi: 10.7717/peerj-cs.814.

[6]G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, “DDoS attacks in cloud computing: Issues, taxonomy, and future directions,” *Computer Communications*, vol. 107, pp. 30–48, Jul. 2017, doi: 10.1016/j.comcom.2017.03.010.

[7]“Azure DDoS Protection—2021 Q1 and Q2 DDoS attack trends,” *azure.microsoft.com*.<https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q1-and-q2-ddos-attack-trends/>

[8]“Indusface,” *Indusface*, Nov. 23, 2020.<https://www.indusface.com/blog/understanding-cloud-ddos-attacks-and-cloud-based-ddos-protection/>

[9]“Cloud DDoS Protection: How to Prevent and Mitigate DDoS,” *www.stormit.cloud*. https://www.stormit.cloud/blog/cloud-ddos-protection-how-to-mitigate-all-risks/ (accessed Dec. 02, 2022)

[10]T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, “A survey of distributed denial-of-service attack, prevention, and mitigation techniques,” *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, p. 155014771774146, Dec. 2017, doi: 10.1177/1550147717741463.