DDoS Attacks in Cloud Computing

Hello!
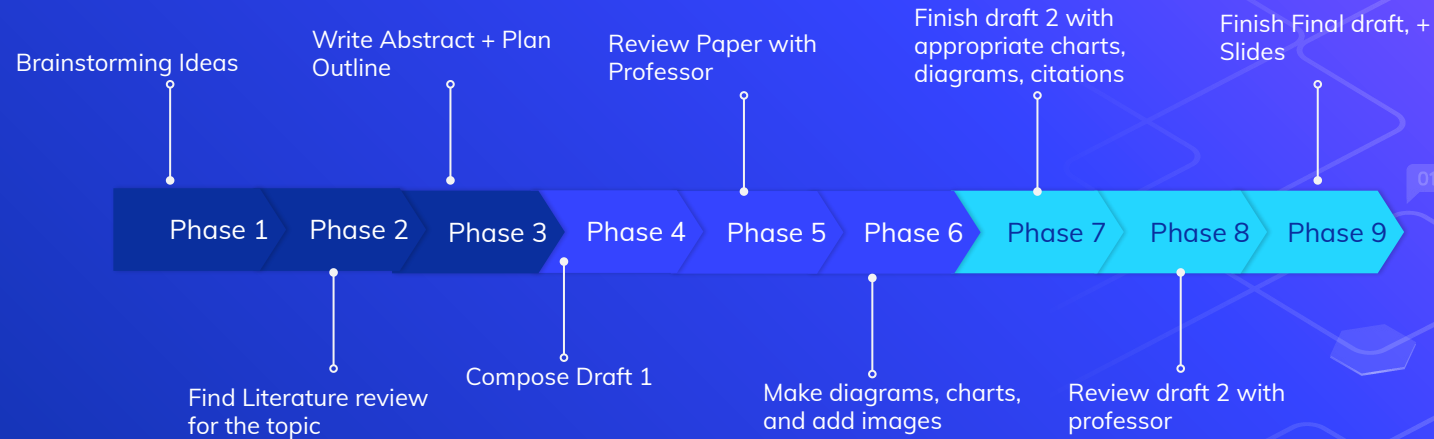
I am Maham Rasheda

Major: Cybersecurity

Minor: Communications

Timeline

Brainstorming Ideas

Write Abstract + Plan Outline

Review Paper with Professor

Finish draft 2 with appropriate charts, diagrams, citations

Finish Final draft, + Slides

Phase 1 Phase 2 Phase 3 Phase 4 Phase 5 Phase 6 Phase 7 Phase 8 Phase 9

Find Literature review for the topic

Compose Draft 1

Make diagrams, charts, and add images

Review draft 2 with professor

Goal of the Research paper

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 .

What is Cybersecurity?

Cybersecurity is the use of various technologies, procedures, and controls with the purpose of defending computer systems, networks, programs, and devices from malicious cyber activity.

History of Cloud Computing

- Cloud computing has started since the 1960s
- 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(Neto)
- In 1990, companies started to offer virtualized private network connections.
- In 2006, Amazon Web Services was created by Amazon.
- It wasn't till 2007 where Cloud Computing started to become more popular.
- In that same year Microsoft launched Microsoft Azure; a cloud computing server to help with management systems.
- Oracle cloud was released in 2016 that provides storage,network, and applications over the internet.

Cloud Computing

Cloud computing is the ability to provide cloud services over the internet.

Layers of Cloud Computing

Platform as a Service(PaaS)

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.

Software as a Service(SaaS)

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.

Infrastructure as a Service (IaaS)

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.
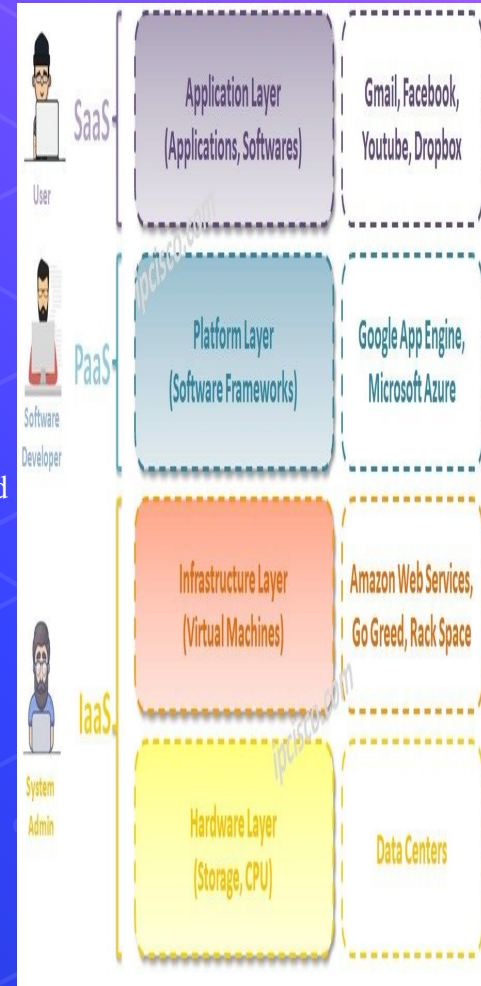
Why is cloud computing useful:

- ⬡ cloud computing is set up makes it financially feasible for businesses to employ it
- ⬡ It enables cost savings in computing and IT
- ⬡ 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.
- ⬡ There are extra security precautions in the cloud, where hosts can specify application security settings and monitor data.
- ⬡ Cloud services enable disaster recovery, which means they can reclaim data in the event of any catastrophe, no matter how big or small.

What are 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.
- ⬡   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.
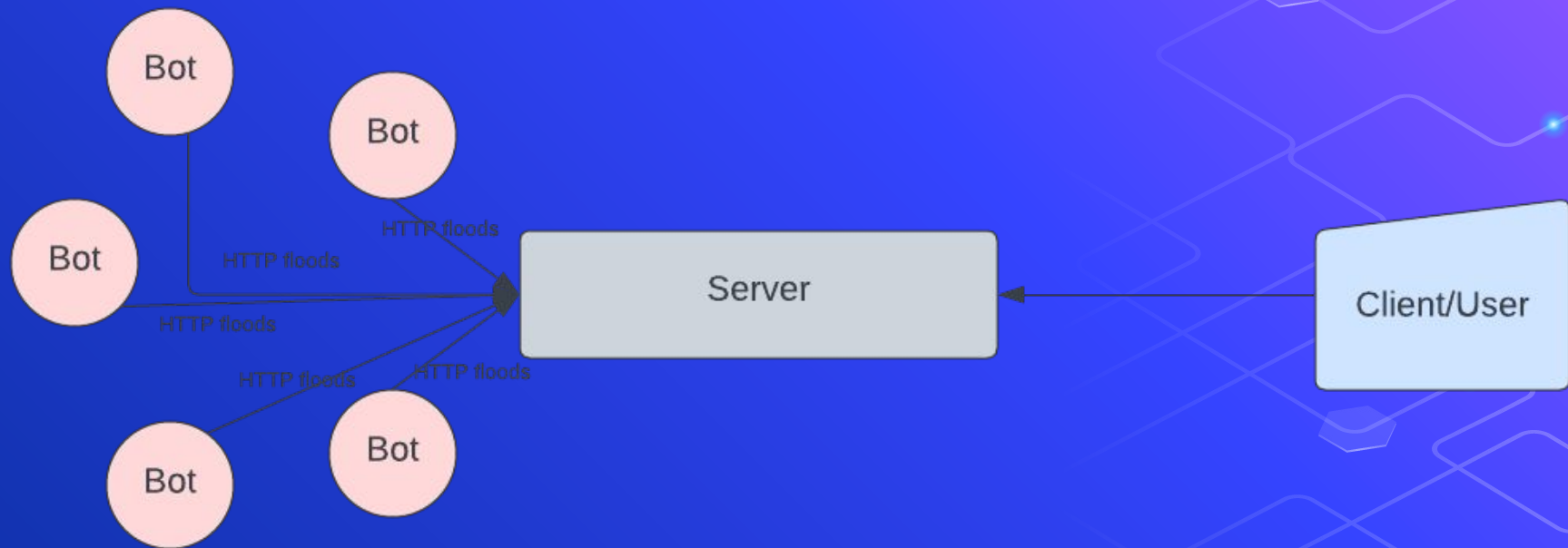- ⬡   It causes data loss, financial data loss, and credibility loss.
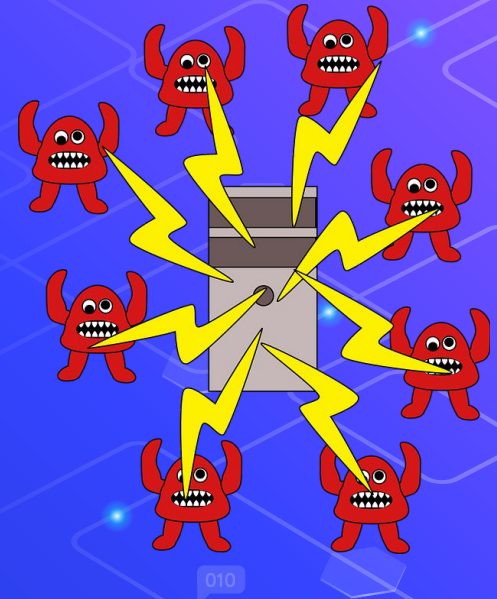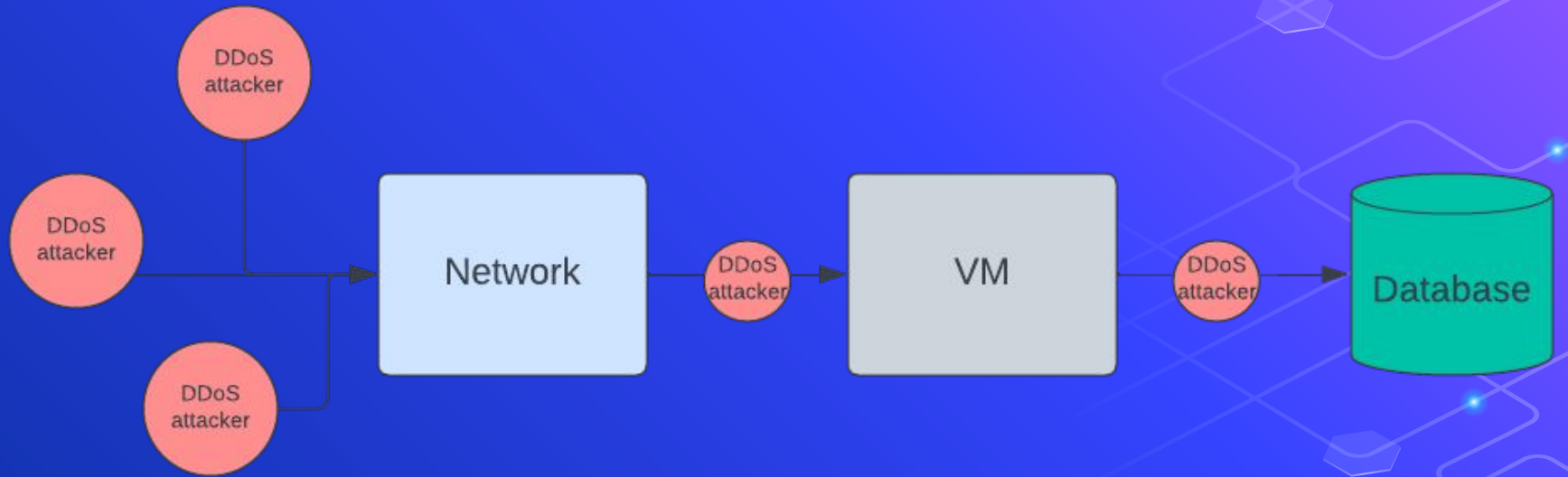
DDoS Attack on the Cloud

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.
- 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

Bot

Bot

Bot

HTTP floods

HTTP floods

HTTP floods

HTTP floods

HTTP floods

Bot

Bot

Server

Client/User

Statistics of DDoS attacks in Cloud Continued

Q1 & Q4 results 2020

○ The figures 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 United States 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.


Q1 results 2020

Q4 results 2020

14
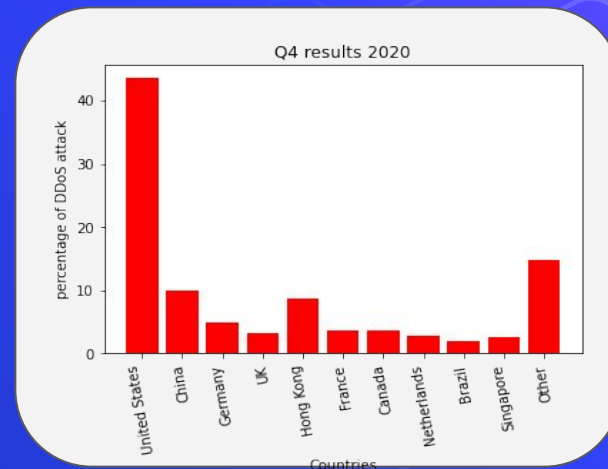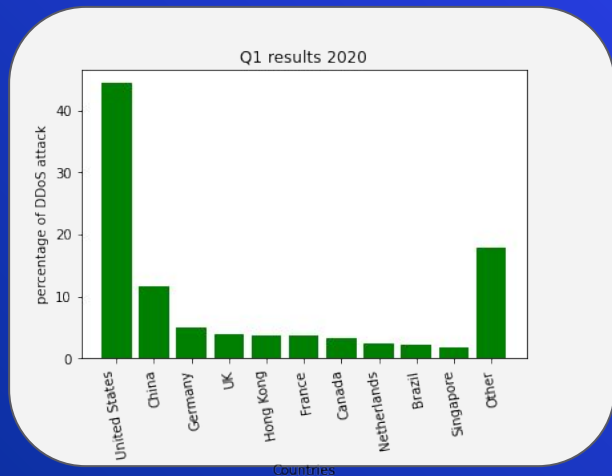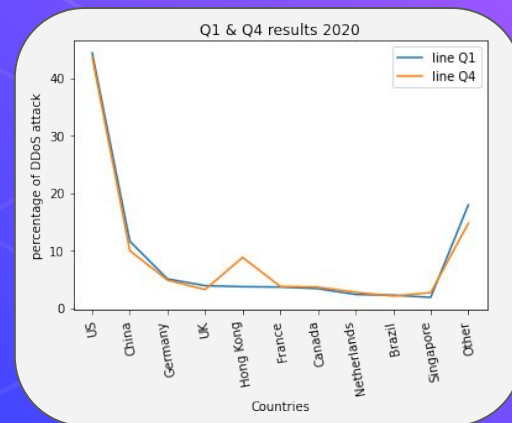
$444,000 USD

Cloud Based DDoS Protecton

- A detection method is one of the things that can be done.
- Ingress filtering stops people from lying about their IP address
- 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
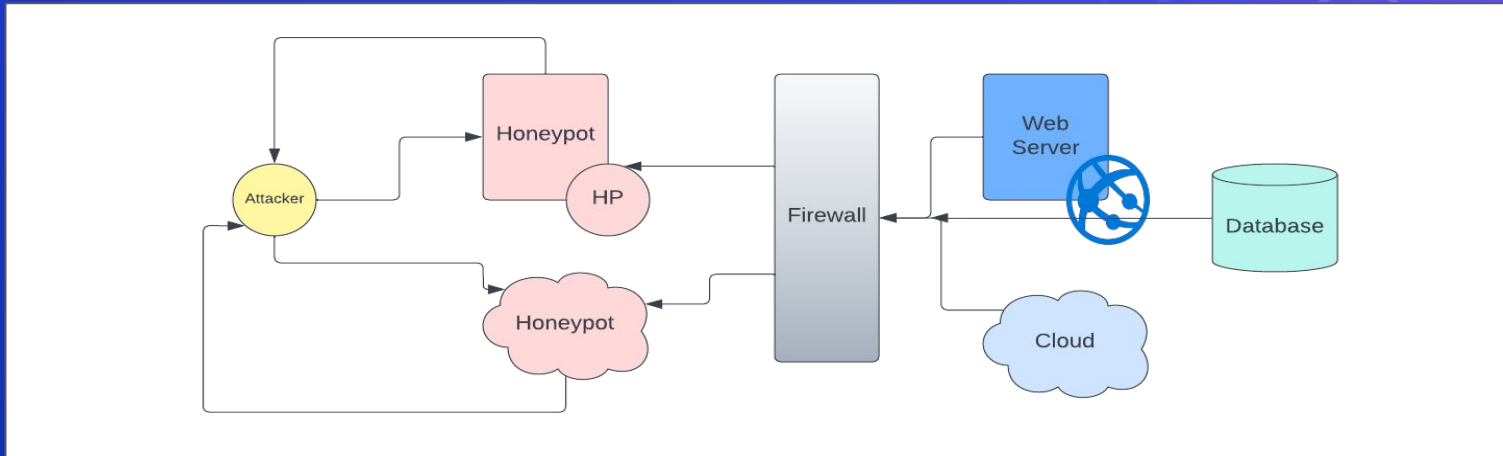
Conclusion

- **Cloud computing no doubt is one of the most groundbreaking and on demand computer systems to be created**
- **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**

❝ Citations:

[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.

Thanks!