Exploring Cloud Computing Challenges: A Thorough Examination of Issues in the Cloud Environment

Vinay Avasthi
Department of Computer Science and Engineering, Himalayan School of Science and Technology, Swami Rama Himalayan University, Dehradun

Abstract- Cloud computing has evolved into a critical component of contemporary enterprises, providing various advantages including scalability, adaptability, and cost efficiency. However, Cloud Computing also introduces a number of security vulnerabilities that can be exploited by cybercriminals. This article provides an overview of the most common cloud vulnerabilities and their impact on cyber security threats. Among various issues, DDoS issue is very serious, so we identify the causes and issues that address these issues.

Keywords: Cloud Computing, Vulnerability, DDoS, Web Service, Domain Name System.

INTRODUCTION

Over the past decades, significant progress has been made in several foundational technological areas, including the data centre, distributed computing, networking, hardware virtualization, etc. One of the new technological subfields that have emerged as a result of these breakthroughs is Cloud computing. Cloud computing describes a computer framework enabling users to access a shared pool of configurable computing resources, including hardware and software, over a network. This access is provided on-demand, with limited intervention required from the service provide [1]. The foundation of Cloud computing was laid in the early 1990s by telecommunication companies with the provisioning of virtual private network services. However, the concept of Cloud computing that we understand today appeared only in the late 1990s. In 1999, salesforce.com first suggested the idea of delivering services to enterprises via the Internet. In 2002, Amazon started Amazon Web Service (AWS) to provide various remote services to enterprises, including storage, computing resources, and business-related services. However, commercial Cloud services became available only in 2006 with the launch of Amazon's Elastic Cloud Computing (EC2), and Google Docs services [2-3].

Ever since its inception, cloud computing has gained widespread attention and support. The rapid adoption of the Cloud computing paradigm can be attributed in large part to its many attractive features, Examples of these features include self-service access as needed, consolidating resources, quick adaptability, and a payment model based on actual usage. Customers of Cloud services and Cloud service providers alike stand to benefit from this concept of cloud computing. Customers can save money on IT costs by using third-party service providers rather than building their systems [4-5].

In addition, the demand for services in organizations that provide web-based ones is notoriously uncertain. As a result, the on-demand functionality of the Cloud enables its users to further cut down on the overall cost of their operations [6-7]. Customers of the Cloud have the option to utilize resources as per their requirements and to pay for those uses under the utility pricing model. Cloud computing aids service providers in minimizing operational expenses, enhancing efficiency, maximizing return on investment, and reducing total cost of ownership [8-9]. It also helps service providers achieve these other goals by lowering their total cost of ownership. In addition to this, it makes the storing of data, the processing of stored data, and the analysis of stored data much simpler [5].

The Cloud model offers an extensive array of features that incentivize organizations to migrate their business operations and data to the Cloud [10]. However, these attributes also create vulnerabilities within the Cloud model. These vulnerabilities are exploited by malicious actors, posing significant security and privacy concerns for data and applications [11]. Among many security and privacy concerns, ensuring

The availability of services and data is paramount. The unavailability of services significantly affects the business and revenue of service providers, frequently prompting customers to switch providers because of poor service quality. In this thesis, we focus on the most challenging reason behind the unavailability of Cloud services: the Distributed Denial of Service attacks. Cloud offers on-demand access to its services. Hence, to disrupt the availability of cloud services, attackers execute well-

Article Received: *25 November 2023* ***Revised:*** *12 December 2023* ***Accepted:*** *30 January 2024*

coordinated Distributed Denial of Service attacks against cloud servers. DDoS [12] attack is the root cause that challenges the availability of services hosted on public Cloud platforms. A Distributed Denial of Service attack aims to disrupt the services of legitimate users either by overwhelming the network bandwidth or by depleting server resources. Such attacks are typically motivated by factors such as financial gain, revenge, ideological beliefs, intellectual challenge, or cyber warfare.

Modern attackers use a botnet to perform complex DDoS attacks. The general method used by attackers to perform these attacks is shown in Figure 1. It depicts to launch a successful DDoS attack; the attacker first recruits some attack handlers. The handlers are recruited by the attacker by first searching the internet for susceptible systems and then installing a handler programme on the systems that have been successfully compromised. Handlers will then begin the hunt for more systems that are susceptible to attack and will install a bot programme on these systems in order to form a botnet. Handlers then give attack instructions to the bots, telling them to launch a distributed denial of service assault against the target server after receiving those instructions from the attacker.

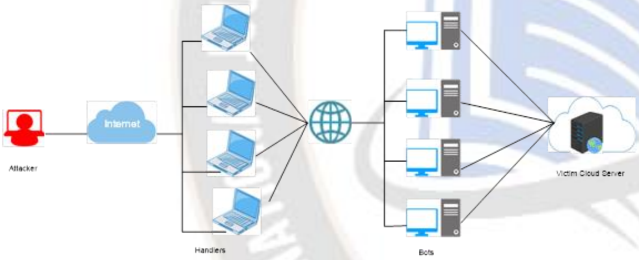

Figure Error! No text of specified style in document.**:** Generalized Model of Distributed Denial of Service Attack

In the past decade, several attacks against major players in the industry are reported. As per the reports published [13-14], “Dyn”, a major Domain Name System (DNS) provider company, experienced a powerful attack having an attack strength of 1.2 Tbps on October 21, 2016, which brings down major websites including Twitter, CNN, Netflix, etc. in Europe and US for the whole day. This attack was performed using the “Mirai” botnet involving 100000 malicious Internet of Things (IoT) devices. This botnet was considered one of the largest botnets of its kind. In another incident, Sony’s Play Station Network (PSN) experienced a attack in August 2014 [15]. This attack prevented the users of PSN from accessing the services. In March 2015, the US coding website GitHub was the target of a large-scale Distributed Denial of Service attack [16]. This attack involved many attack vectors, including previously seen attack vectors and some new sophisticated techniques as well.

ISSUES AND CHALLENGES IN CLOUD COMPUTING

The Cloud computing model is not a completely new computing platform. It can be considered an intelligent integration of various technologies, including distributed computing, networking, data center technology, etc. Therefore, it inherits several security challenges from its parent technologies. However, it also suffers from several new security challenges. Our research is motivated by the following factors.

Challenges in the adoption of public Cloud computing platform

Enterprises have several concerns in adopting the public Cloud computing platform. One important concern is the availability of data and services hosted on the Cloud. The Cloud platform needs to assure that the services are available to the enterprises uninterrupted and persistently. One of the fundamental functions of Cloud computing is to provide various Cloud services on-demand; therefore, ensuring the availability of services becomes more crucial in Cloud computing. If a specific service becomes unavailable for a longer period or the QoS does not qualify the expectations of Cloud customers, then customers may lose trust in the Cloud service provider and may also move to another Cloud service provider. The availability of services in Cloud computing is mainly challenged by DDoS attacks. The DDoS attacks on Cloud computing have several negative implications and mitigation of these attacks is challenging as well.

Difficulties in attack detection and mitigation

Managing the detection and mitigation of DDoS attacks presents numerous technical challenges, which encompass the following:

- ***The large number of bots in the botnet:*** Modern botnets typically comprise a significant number of bots. This obviates the necessity for attackers to spoof source IP addresses. This makes the DDoS defense mechanisms based on spoofed source IP addresses ineffective. Moreover, it also makes the detection of DDoS attacks more complicated as the attack traffic generated by modern botnets looks similar to legitimate traffic.
- ***DDoS attacks mimicking flash crowd events:*** To avoid detection, DDoS attackers attempt to mimic the attack traffic as flash crowd events. Hence, many times DDoS attack traffic may be classified as flash crowd traffic and vice versa.
- ***Attacks targeting Cloud’s fundamental features:*** Cloud’s fundamental features including the pay-as-you-go pricing model, multi-tenancy, etc. can be targeted by

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 2
***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

adversaries to perform DDoS attacks on Cloud computing.

- ***Challenges arise in maintaining the desired Quality of Experience during the attack:*** During DDoS attacks, the server resources are exhausted by the attack packets; therefore, a legitimate user`s Quality of Experience (QoE) degrades significantly. Hence, it is a challenge to maintain the desired user's QoE during these attacks.
- ***High false positive/ false negative rate:*** To reduce the attack impact, timely detection and mitigation of DDoS attacks are expected. However, detecting these attacks in less time results in the misclassification of legitimate packets as attack packets and vice versa. Hence, it is desired to reduce the false positive rate/false negative rate while detecting DDoS attacks.

Increased Attacks on Cloud Computing

The intensity and impact of DDoS attacks are escalating over time. According to a report on DDoS attacks [16], The prominent Cloud service provider experienced a notable surge in DDoS attacks compared to previous periods. Figure 2 shows the Q3 2022 DDoS attacks. After dropping 13.72 percent in the previous quarter, it plunged 27.29 percent to 57,116. Kaspersky's DDoS Intelligence system detected 824 attacks per day in August [17]. In July, 45.84% of all assaults occurred in the first week, keeping June's average of 1301 per day; after week two, the average number of daily attacks declined to 448. July averaged 641 DDoS attacks per day, marginally behind September's 628.5. September's attacks were more evenly spread.

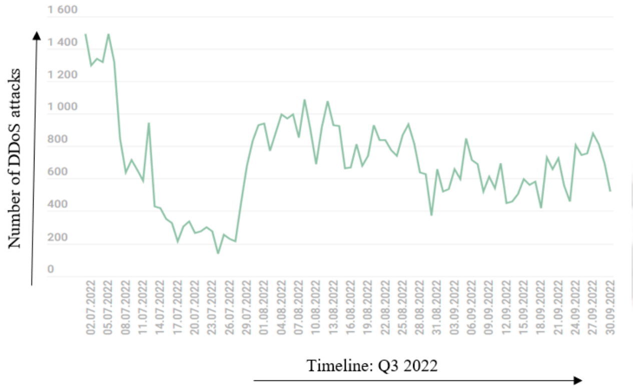

Figure1: The intensity and impact of DDoS attacks during Q3 2022

This quarter it fell by 27.29 percent, to 57,116, after falling 13.72 percent in the prior quarter. August was the busiest month, with an average of 824 attacks per day. July was calm: 45.84% of all attacks occurred in the first week, maintaining June's average of 1301 per day; after week two, the average number of daily attacks dropped to 448. In July, there were 641 DDoS attacks per day and more than 628.5 in September.

The most violent day was July 1 (1494 attacks), while the calmest was July 24. (135). In August, the 8th and 12th had over a thousand attacks each, and the 30th was the quietest day (373). July 1 was the most aggressive day (1,494 attacks); July 24 was the calmest (135). The 8th and 12th of August had over 1,000 attacks each, and the 30th was the quietest (373). September was uneventful. Figure 3 shows the percentage of DDoS. Botnet servers are still mostly in the US (43.10%), although their share declined by 3%. The Netherlands (9.34%) fell more than 5 percentage points and was replaced by Germany (10.19%). Fourth-place Russia (5.94%) remained [17].

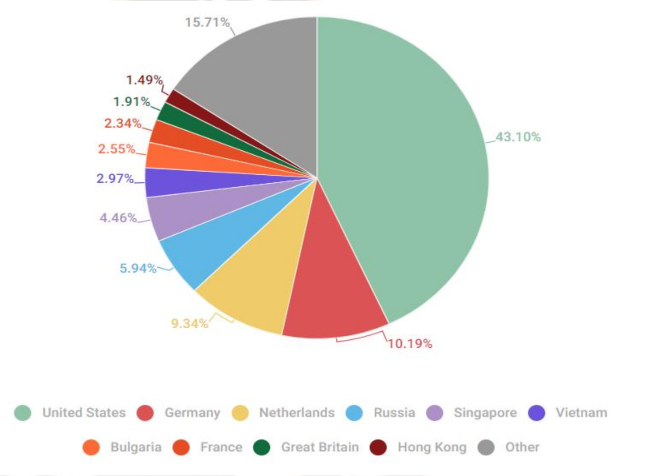

Figure 2: Impact of DDoS attack in the year 2022

Asian countries follow Singapore (4.46%) and Vietnam (2.97%), whose proportion in Q3 grew, although not as quickly as in Q2. Bulgaria (2.55%), a new entrant, increased its share more than sixfold. France (2.34%) and the UK (1.91%) fell from fifth to eighth and ninth, respectively. Canada and Croatia, last quarter's TOP 10, lost C2 servers to Hong Kong (1.49%). Figure 4 Indicates the distribution of DDoS attacks across various industries [18].

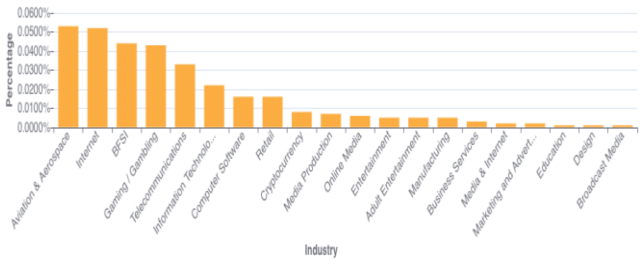

Figure 3: Distribution of DDoS attacks across various industries

Article Received: *25 November 2023* ***Revised:*** *12 December 2023* ***Accepted:*** *30 January 2024*

In fig 5 compare the percentage of DDoS attacks in Industry (Quarterly) during 2022. It clearly shows that there is a significant increase in the DDoS attack rate in the industry [18]. They further reported in 2022 that 52% of DDoS attack mitigations done on behalf of its customers were for the IT/Cloud industry.

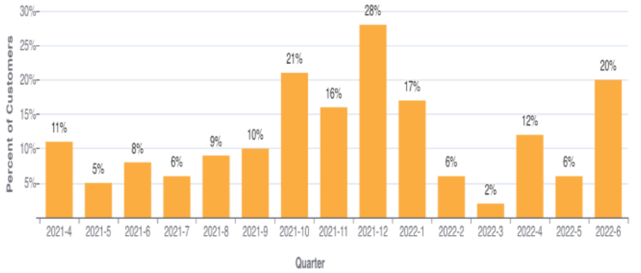

Figure 4: Compares the percentage of DDoS attacks in Industry (Quarterly) during 2022

Figure 6 An attack vector refers to the method utilized by an attacker to execute their DDoS attack, encompassing factors such as the IP protocol, packet characteristics like TCP flags, flooding techniques, and other criteria [18]. DDoS assault vectors displays the number of methods that can be used to carry out a DDoS assault. Some of these methods include SYN, DNS, RST, UDP, and TCP, amongst others.

In the second quarter, SYN floods represented 53 percent of all network-layer attacks. Flooding using SYN packets continues to be the most common form of assault. They make improper use of the stateful TCP connection request during the handshake's initial phaseWhen he initiates his initial connection request the servers lack context regarding the TCP connection as it is fresh and new. Without the appropriate safeguards, it may be difficult for servers to prevent a flood of initial connection requests from being made. This makes it much simpler for the adversary to utilise the resources of a server that is not protected. Following the SYN floods come assaults directed against the DNS system, RST floods that abuse the flow of TCP connections, and general attacks carried out using UDP.

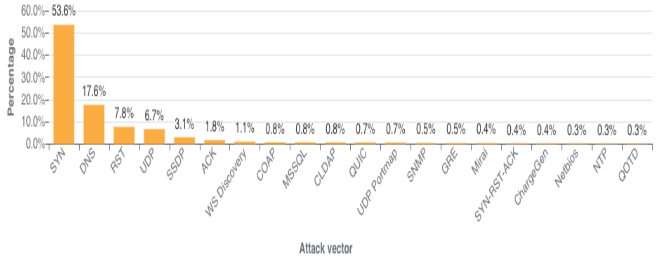

Figure 5: DDoS attack vector

FINANCIAL IMPLICATION OF DDOS ON CLOUD COMPUTING

DDoS attacks have negative financial implications on Cloud service providers as well as on enterprises hosting their services on Cloud. As services are interrupted due to DDoS attacks, it may result in a huge financial loss. Enterprises and users keep their sensitive and confidential data on the public Cloud. Apart from affecting the availability of Cloud hosted services, DDoS attacks may also lead to data loss which can further attract financial and legal liabilities. In Cloud computing, the DDoS attack is performed to challenge the victim's ability to host web services on a public Cloud platform for the long term.

CONCLUSION

Cloud computing provides numerous advantages for businesses regardless of their size. However, it's crucial to recognize the security vulnerabilities linked with cloud computing and implement suitable mitigation strategies. We have performed a comprehensive literature review to point out various merits and limitations of cloud computing and challenges in the detection and mitigation of attacks in a Cloud environment. In this article, we have outlined the concerns and challenges present in cloud computing.

REFERENCES

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, U.S Department of Commerce, Computer Security Division, Information Technology Laboratory, NIST Special Publication, 2011.

[2] The History of Cloud Computing, https://www.eci.com/cloudforum/cloud-computing-history.html, [Accessed on 4/09/2023]

[3] M. D. Neto, "A brief history of cloud computing", https://www.ibm.com/blogs/cloud-computing/2014/03/a-brief-history-of-cloud-computing-3/, [Accessed on 4/09/2023]

[4] Gu, J., Anjum, A., Wu, Y., Liu, L., Panneerselvam, J., Lu, Y., & Yuan, B. (2022). The least-used key selection method for information retrieval in large-scale Cloud-based service repositories. Journal of Cloud Computing, 11(1), 1-19.

[5] Erkin, Z., Veugen, T., Toft, T., & Lagendijk, R. L. (2013). Privacy-preserving distributed clustering. EURASIP Journal on Information Security, 2013(1), 1-15.

[6] R. Buyya, J. Broberg, A. Goscinski, "CLOUD COMPUTING: principles and paradigms", John Wiley & Sons, Hoboken, 2011.

***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

[7] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.

[8] Qu, Z., Dawande, M., & Janakiraman, G. (2022). Cloud Cost Optimization: Model, Bounds, and Asymptotics. Bounds, and Asymptotics.

[9] Makhlouf, R. (2020). Cloudy transaction costs: a dive into cloud computing economics. Journal of Cloud Computing, 9(1), 1-11.

[10] Kritikos, K., Zeginis, C., Iranzo, J., Gonzalez, R. S., Seybold, D., Griesinger, F., & Domaschka, J. (2019). Multi-cloud provisioning of business processes. Journal of Cloud Computing, 8(1), 1-29.

[11] Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: technical review. Future Internet, 14(1), 11.

[12] Gupta, Brij & Dahiya, Amrita. (2021). Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges, and Countermeasures. 10.1201/9781003107354.

[13] Kyle York, “Dyn Statement on 10/21/2016 DDoS Attack”. [online] https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/ [Accessed on: 5/09/2023], 2016.

[14] Scott Hilton, “Dyn Analysis Summary Of Friday October 21 Attack”, [online] https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ [Accessed on: 5/09/2023], 2016.

[15] Fred Dutton, “PlayStation Network is back online (update)”, https://blog.eu.playstation.com/2014/08/24/playstation-network-update/, [Accessed on 6/09/2023], 2014.

[16] Jesse Newland, “Large Scale DDoS Attack on github.com”, https://github.com/blog/1981-large-scale-ddos-attack-on-github-com, [Accessed on 6/09/2023], 2018

[17] Oleg kupreev, alexander gutnikov, yaroslav shmelev, “DDoS Attack in 2022”, https://securelist.com/ddos-report-q3-2022/107860/, [Accessed on 6/09/2023], 2022

[18] Omer Yoachimik, “DDoS attack trends for 2022 Q2”, https://blog.cloudflare.com/ddos-attack-trends-for-2022-q2/, [Accessed on 7/09/2023], 2022