CEPAT Journal of Computer Engineering: Progress, Application and Technology
Vol. 1, No. 2, November 2022, pp. 108-117
ISSN: 2963-6728, DOI: https://doi.org/10.25124/cepat.v1i02.5269

5G Mobile Private Security Analysis Based on Cloud Computing

Michelle Octavia Yolanda Sari[1], Rendy Munadi[2], Fardan[3]
[1,2,3]Department of Telecommunication Engineering, School of Electrical Engineering, Telkom University, Indonesia

Article Info

Article history:

Received August 12, 2022
Revised August 15, 2022
Accepted August 19, 2022

Keywords:

5G Network
Telco Cloud
Distributed Denial of Service
Private Cellular
Network Function Virtualization

ABSTRACT

As time passes by, the increasing demands from 4G technology services to 5G technology are getting bigger. In line with the development of 5G, there are several open sources such as Free5gc, Open5gs which already provide core 5G network services so that they can help create and simulate private 5G networks. By using free5gc open source, it still needs more attention from the security side, especially from common attacks such as DDoS. Then the attack scenario is carried out from the inner network side, namely from the UE with the TCP SYN Flood and Ping of Death attack methods. The results of the attack contained comparisons for CPU and memory usage parameters. Then the TCP SYN Flood attack had an impact for CPU usage with an average result cpu usage of 2,74% and on the core network function components, namely Access and Mobility Management (AMF), which in 5G services experienced errors or crashes after receiving large packets. Thus, users cannot use the service because if an error occurs in the core network function (AMF), then the connection to gNB and the UE will also be lost.

Corresponding Author:

Michelle Octavia Yolanda Sari
Department of Telecommunication Engineering
School of Electrical Engineering, Telkom University
Bandung, Indonesia
Email: michelleoctavia@student.telkomuniversity.ac.id

1. INTRODUCTION

1.1. Overview Network Nowadays

As time passes by, telecommunication becomes one of the vital aspects in human life. Starting from 1G until now to 5G signifies a great influence in daily human activities and also, 5G becomes very important for technological progress in the world, especially Indonesia [1]. With this influence, it is meant that the development of 5G in terms of services, security, infrastructure, and any other facilities will be more effective by allowing many people to deliver things more quickly and comfortably. The advantages offered by 5G are higher bandwidth and lower latency [2]. Then, based on 5G PPP or 5G Public Private Partnership in 2015 stated that 5G technology has a vision to make technology a key in the digital world with support from ultrahigh band infrastructure for all fields and levels in the market [1].

Currently, various agencies have begun to develop simulations of 5G networks, both open source and commercial. The open source created is used for simulation on the core network side and simulation on the User Equipment (UE) and RAN sides. In its further development, 5G is also directed to be carried out in the form of virtualizing its network functions or commonly called NFV [3]. NFV can improve network elasticity, simplify network control and management, and thus be considered very important for future networks. To build this private 5G cellular network with the CONCEPT of NFV, a container is needed for the core network, such as cloud computing services [4] [5] [6].

Since its inception, mobile networks have been vulnerable to security vulnerabilities [6]. With the advent of fifth-generation (5G) wireless networks, the security threat vector will become larger than ever with greater attention to privacy. There are some basic 5G challenges such as flash network traffic, DoS attack on the infrastructure, and any other variables. Thus, the authors propose an analysis on 5G security parameters using the Free5GC simulator and UERANSIM simulator using DDoS attack experiments with various types of methods in DDoS in Cloud Computing services. This research is expected to be a reference for anyone who wants to implement 5G networks privately, considering the lack of references to this research.

1.2. Cellular 5g Network

Wireless cellular technology has transitioned from the first generation to the next generation for ten years [7]. Today we are about to embrace the 5G, fifth generation of cellular network. The transition of mobile networks from 3G/4G to 5G will lead to a very profound change as users make many requests that require new approaches to connectivity, bandwidth, and network architecture issues. Evolution on 5G networks will include both physical and virtual functions and this will eventually be deployed in the cloud. Due to this circumstance, NFV or Network Functions Virtualization is very important in 5G network deployment, because it will help to reduce operating costs and provide more values to network infrastructure [8]. With the presence of 5G technology, it is meant to provide major changes for the industry. Especially in Indonesia, it is also expected to have a significant impact on the use, focusing on private 5G technology. The latest technological developments have made it possible for the unification of telecommunications and cloud. The unification of these two infrastructures can help achieve good performance as it can be the basis for transforming a telecommunications company into a digital service provider and reduce operating costs. 5G also has a core network that allows it to support its functionality, in **Fig. 1** shows the 5G core network architecture, namely NEF (Network Exposure Function), NRF (Network Function Repository), PCF (Policy Control Facility), UDM (Unified Data Management), AUSF (Authentication Server Function), SMF (Session Management). Function), UPF (User Plane Function), AMF (Access and Mobility Management) [7].

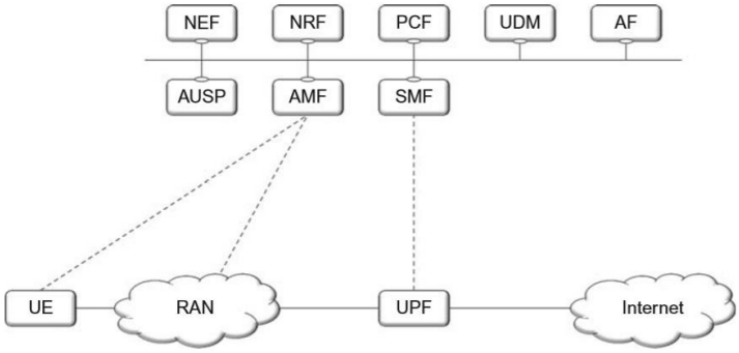


Fig. 1 5G Core Network Architecture

1.3. Telco Cloud

The definition of Telco Cloud in general is an infrastructure consisting of a Mobile Device (MD), access network, sensors, Internet, and Data Center (DC) [9]. By using Telco Cloud, the concept of virtualization can be applied from the data center into the network. Especially in 5G technology, telco cloud itself will be more built on container technology and when it uses telco cloud, it must also be side by side with Network Function

Virtualization or NFV [4] [10]. However, the Telco Cloud concept itself still has problems, namely unstable in the term of Quality of Service (QoS), precisely instability in latency. **Fig. 2** shows the Telco Cloud Scheme

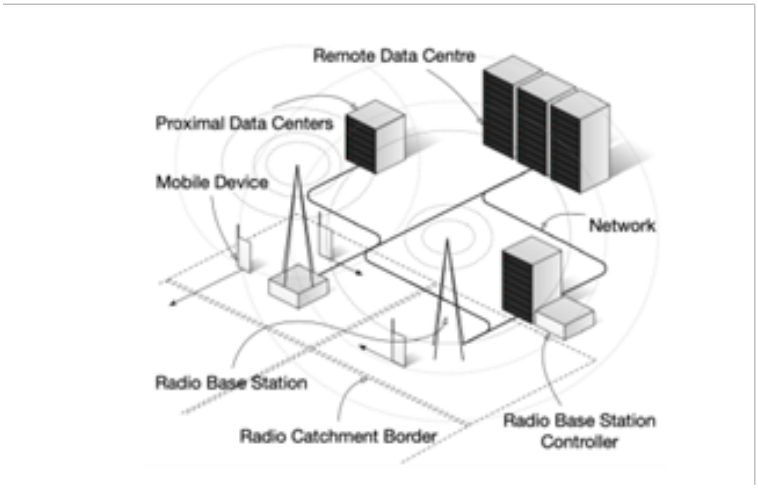


Fig. 2 Telco Cloud Scheme

1.4. Private 5G Network

The presence of the latest 5G network technology is expected to provide major changes and high performance. This expectation comes from user requests such as low latency, stable connectivity, can transfer more data. Even though it has made the desired impact and performance, the telecommunications industry wants to optimize the 5G network by using 5G private network technology. Private network technology is a non-public cellular network, 5G private Network is a network that is specially created by offering a level of reliability, security, and provides many valuable benefits such as more efficient, scalable, and inexpensive marketing time [11].

1.5. Network Function Virtualization

Network Function Virtualization (NFV) is a concept or idea raised by internet service providers that aims to transform service providers and develop virtualization technology and can be implemented in the form of software defined that runs on industry [4] standard hardware Research on NFV began with the concept of cloud computing by virtualizing a hardware and developing it into an infrastructure, platform, and software. ETSI or European Telecommunication Standards Institure has a standard for nfv design design which is divided into three elements [4] as shown in **Fig. 3** namely NFVI, NFV MANO, and VNF s.

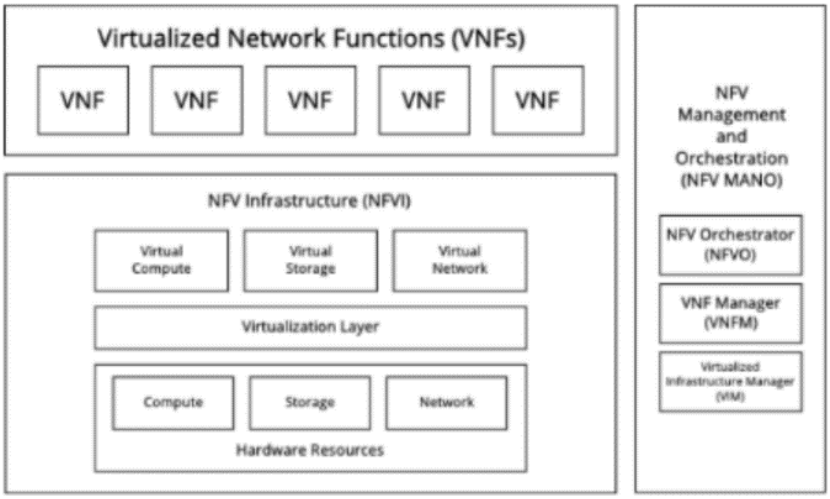


Fig. 3 NFV Architecture

2. PROPOSED MODEL EXPERIMENT

2.1. Overview Model

In this research, the process of building a 5G standalone (SA) network has two components that are important to separate the inside of the 5G core network. The two components are the Control Plane and the User Plane. The Control Plane includes everything in the core network from AF, UDM, PCF, NRF, NEF, NSSF, AUSF, AMF, and SMF. After that, each component of the control plane is connected to the UPF. The UPF is also connected to Radio Access Network (RAN) and UE (User Equipment) in the core network access network domain and belongs to the core network User Plane domain. After everything is successfully integrated, it connects the access network from the EU simulator. All components in the core and access network are stored in two virtual machines which will be deployed through cloud computing and stored through the cloud service platform, Microsoft Azure as shown in **Fig. 4**. In the system model or deployment design, the 5G network security parameters will then be measured. The results of this experiment will be a benchmark for the authors to measure the performance results of each parameter that has been determined in the service scenario in Microsoft Azure. Then, there is also the difference in merging or peering for virtual networks. This affects the data packets sent because the schema in the cloud is different from the network path schema on the local computer.

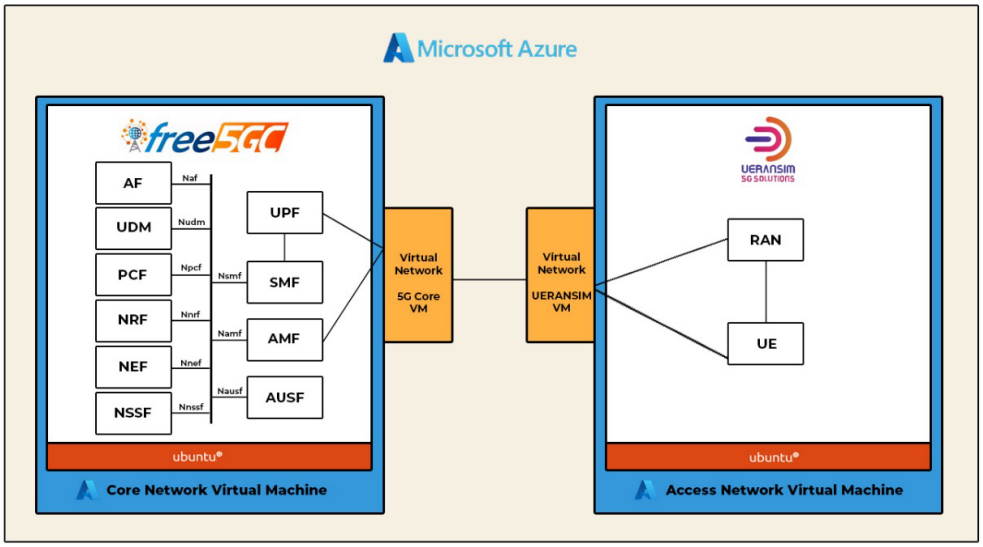


Fig. 4 5G Private Model in Cloud Coputing Platform

2.2. DDoS Penetration Testing

Distributed Denial of Service (DDoS) is an attack or threat to disrupt the normal traffic of a target server, service, or network by flooding the target or surrounding infrastructure with heavy Internet traffic [14]. DDoS attacks achieve their effectiveness by exploiting some compromised computer systems as a source of attack traffic. The exploited machines can include other network resources such as computers and IoT devices. In general, DDoS attacks are like unexpected traffic jams that clog highways and prevent normal traffic from reaching its destination. In this research, DDoS penetration was carried out to find out whether this attack will reduce the performance of 5G networks which are deployed by using the free5GC open source application. The parameters for this experiment are CPU Usage, Memory Usage.

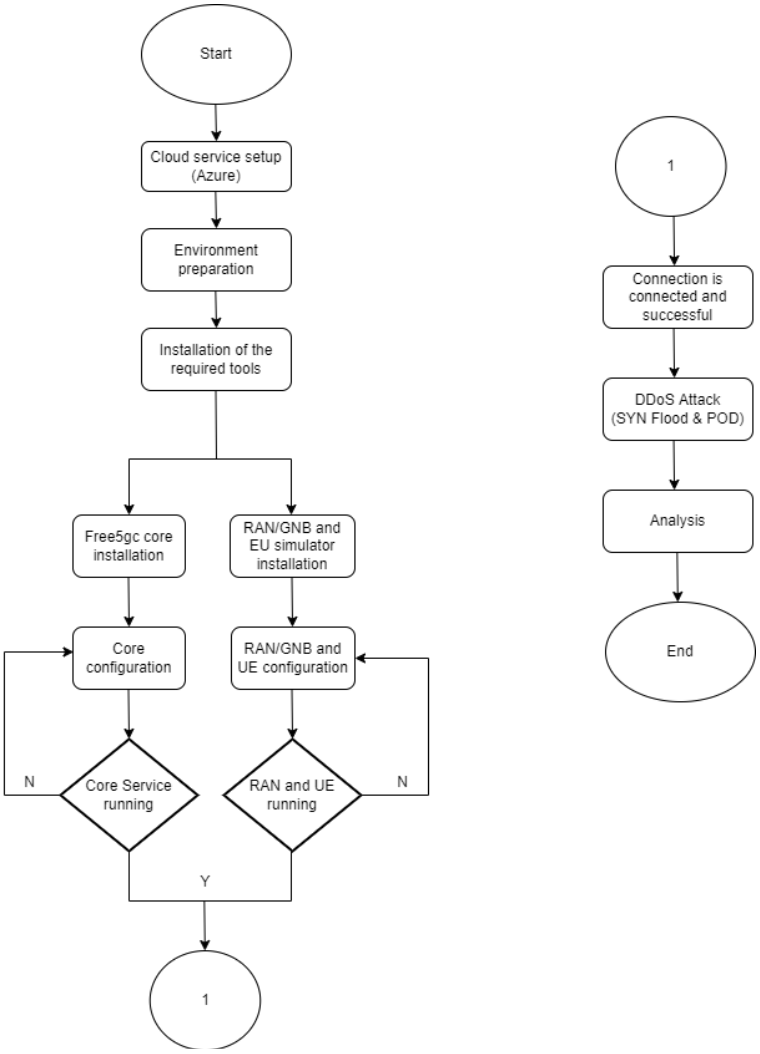


Fig. 5 Flowchart Model

CPU Usage is a parameter used to determine the capacity or speed of the CPU used. Memory Usage is a parameter used to determine the availability of RAM memory used. In brief, proposed model flowchart can be seen in **Fig. 5**.

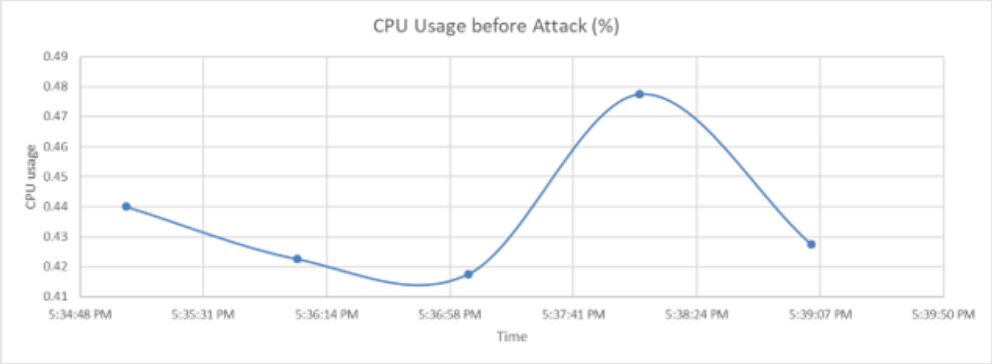
3. RESULTS AND DISCUSSION

Result of this experiment, especially on DDoS penetration testing utilized by using TCP SYN Flood and Ping Of Death (POD). The results will show before and after penetration on each performance parameters which are proposed.

3.1. Result on TCP SYN Flood Penetration Testing

In this scenario, it will be done using the syn flood method from the UE. The TCP SYN flood process is where the attacker quickly initiates a connection to the server without completing the connection.

(a)



(b)

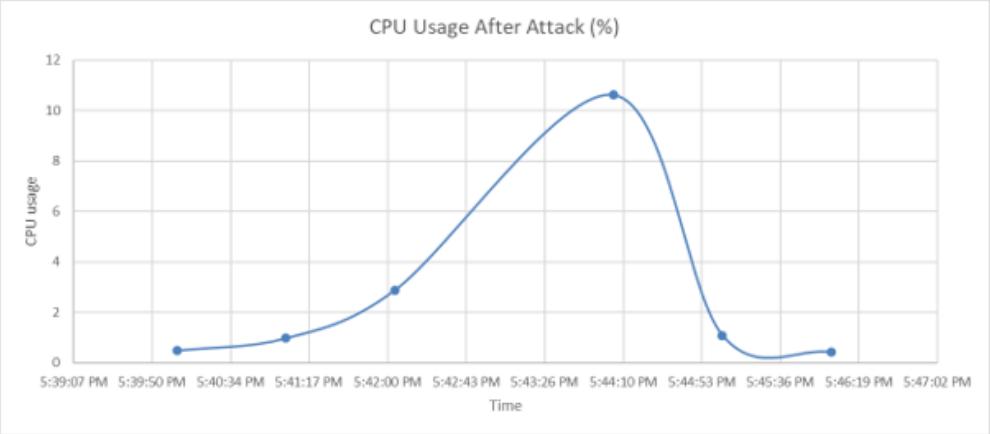
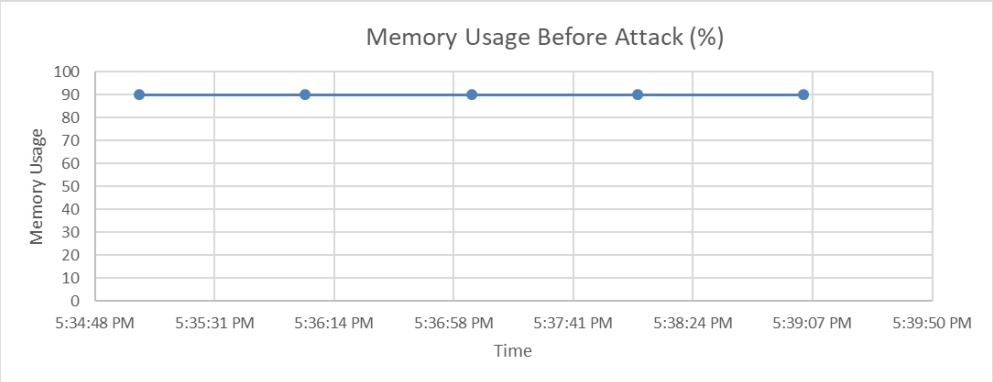


Fig. 6 Performance Results on CPU Usage from TCP SYN flood: a) performance before attack on cpu usage; b) performance after attack on cpu usage.

(a)



(b)

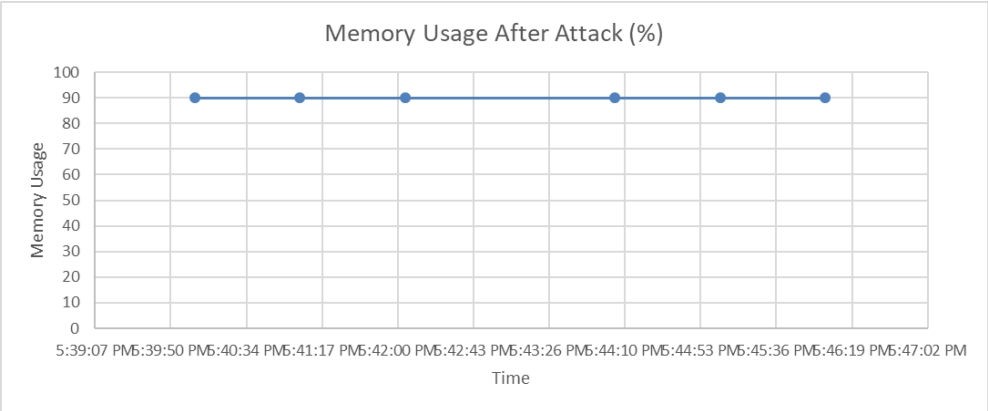


Fig. 7 Performance Results on Memory Usage from TCP SYN flood: a) performance before attack on memory usage; b) performance after attack on memory usage.

Based on results shows on **Fig. 6** shows the monitoring of the Free5GC server which is the victim in this test. The data above shows the cpu usage before the SYN flood attack and the average cpu usage is 0,437%. Then, in **Fig. 6** shows the change in the performance of the server after being hit by a SYN flood attack, which is 2,74%. This change occurs because the power consumption on the server also increases in CPU usage. This increase in activity can indicate that a simulated attack has been launched.

In the next parameter, the memory usage in **Fig. 7** before the attack was 90%. Then, in after an attack, memory usage did not change or could be said to be stable at 90%.

However, it turns out that the attack from the UE side does not only interfere with the use of CPU, memory. As seen in **Fig. 8**, the AMF network function has an error when it is attacked so that gNB and UE cannot connect to the core either.

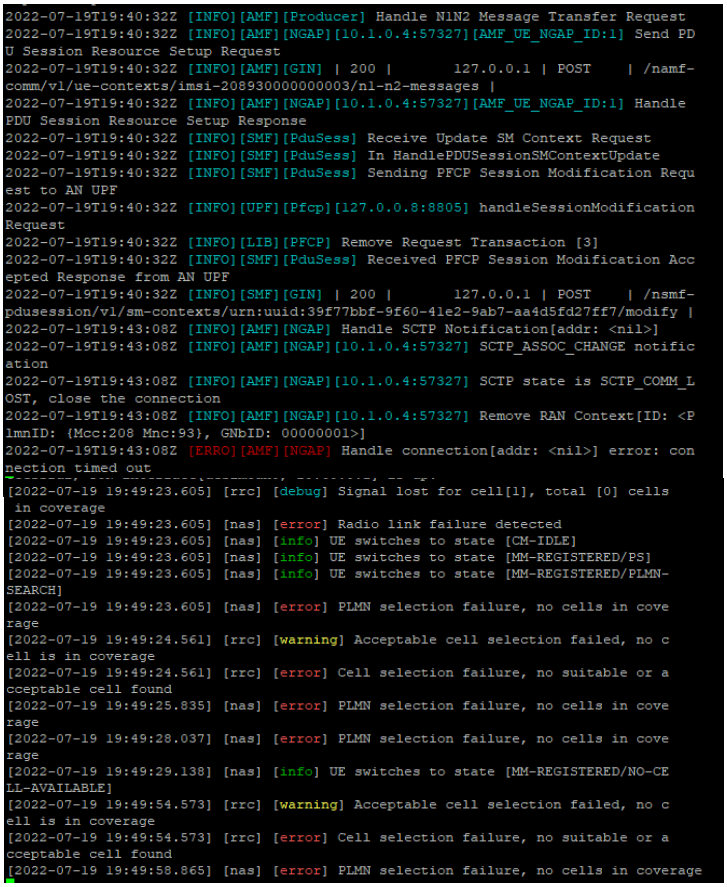
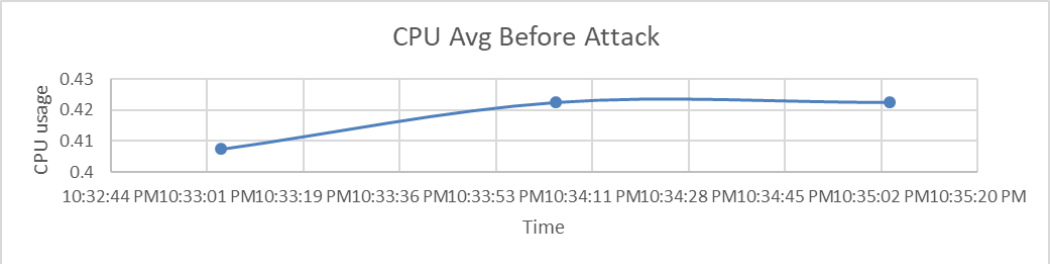


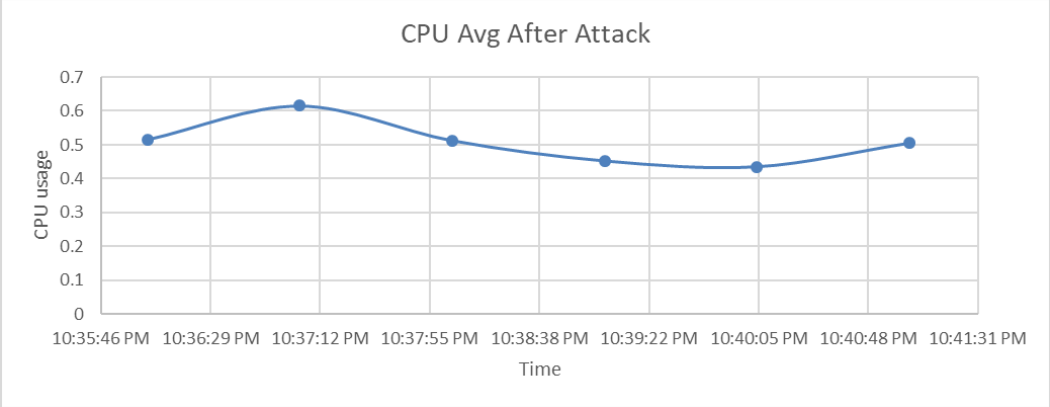
Fig. 6 Result on AMF Error

3.2. Result on Ping of Death Penetration Testing

Fig. 9 shows the change in the performance of the server after being hit by a Ping of Death attack, which is 0,5%. From these data it shows that the effect of Ping of Death attacks on CPU usage is not as big as that given by TCP SYN flood attacks.



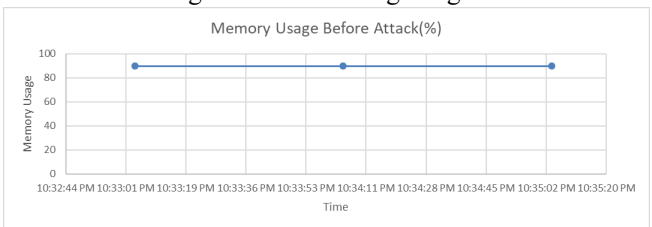
(a)



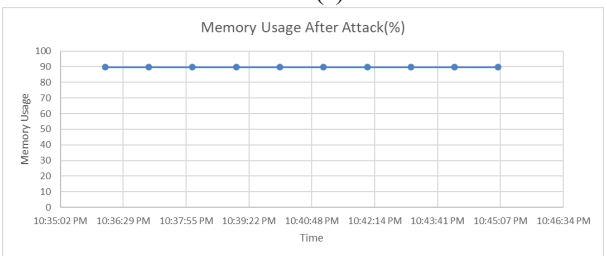
(b)

Fig. 7 Performance Results on CPU Usage from Ping of Death: a) performance before attack on cpu usage; b) performance after attack on cpu usage.

The memory usage parameters can be seen in **Fig. 10**, The data shows that memory usage is also stable from before and after being given a Ping of Death attack. However, from the data it is also seen that the memory usage when getting a Ping of Death attack is greater than when getting an attack from a TCP SYN flood.



(a)



(b)

Fig. 8 Performance Results on Memory Usage from Ping of Death: a) performance before attack on memory usage; b) performance after attack on memory usage.

3.3. Comparison Result

(a) (b)

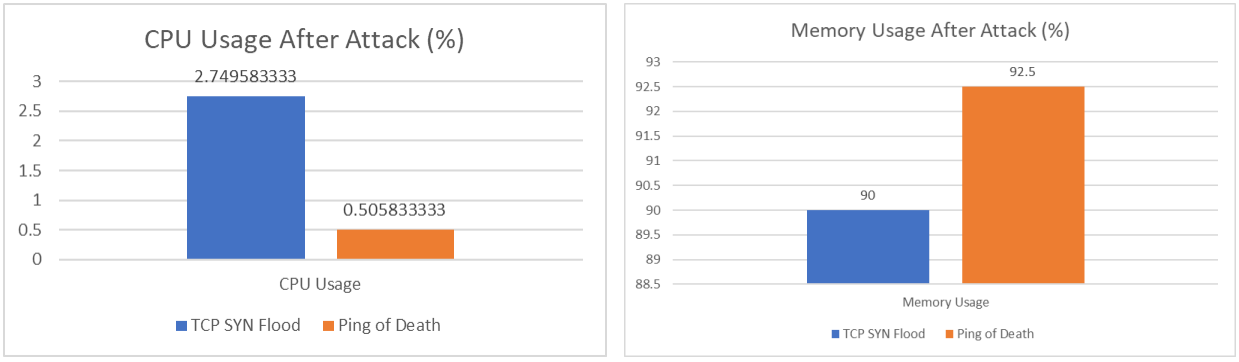


Fig. 9 Performance evaluation of a secure 5G: a) performance comparison of cpu usage from tcp syn flood; b) performance comparison of memory usage from ping of death

Comparison of CPU usage when there is a SYN attack the results are greater than Ping of Death attacks. The average value that can be seen from the **Fig. 11** is that the SYN attack is 2.74% and Ping of Death is 0.5%. Then for memory usage, in the **Fig. 11** shows that Ping of Death attacks are more influential to have an impact on memory usage. The results obtained from each, namely, the SYN attack with an average value of 90% and the average value of Ping of Death is 92.5%.

4. CONCLUSION

Based on research that has been done, cloud computing-based 5G networks are still vulnerable to DDoS attacks, this can be seen from the results of penetration testing which show an anomaly after DDoS attacks are deployed. DDoS attacks have a significant effect on the network, especially on network functions, especially in tcp syn flood attacks, with an average cpu usage result of 2.74% and there is an error in the amf network function, so in the future there must be a security system for 5G considering the performance after testing, so that when it comes to commercialism 5G networks are ready for mass use..

ACKNOWLEDGEMENTS

The author would like to thank those who have helped in the preparation of this article so that it can be published and add references in the field of private 5g cellular networks, especially in security.

REFERENCES

[1] A. Wijaya, "Perkembangan Teknologi 5G," *Univ. Pendidik. Indones.*, vol. 1, no. 1, pp. 2–5, 2021.

[2] K. Dewi, "Teknologi 5G," *Artik. Mhs. Sist. Telekomun.*, no. 1, pp. 1–3, 2021, doi: 10.13140/RG.2.2.35839.02727.

[3] Z. Salazar, H. N. Nguyen, W. Mallouli, A. R. Cavalli, and E. M. Montes De Oca, "5Greplay: A 5G Network Traffic Fuzzer - Application to Attack Injection," *ACM Int. Conf. Proceeding Ser.*, vol. 1, no. 1, pp. 1–12, 2021, doi: 10.1145/3465481.3470079.

[4] M. Fadhil, E. P. Nugroho, Y. Wibisono, and I. Z. Abdillah, "Perancangan dan Implementasi Network Functions Virtualization (NFV) Berbasis Cloud Computing dengan OpenStack," *JATIKOM J. Teor. dan Apl. Ilmu Komput.*, vol. 1, no. 2, pp. 85–90, 2018.

[5] S. Zhang, Y. Wang, and W. Zhou, "Towards secure 5G networks: A Survey," *Comput. Networks*, vol. 162, p. 106871, 2019, doi: 10.1016/j.comnet.2019.106871.

[6] A. Dutta and E. Hammad, "5G Security Challenges and Opportunities: A System Approach," *2020 IEEE 3rd 5G World Forum, 5GWF 2020 - Conf. Proc.*, pp. 109–114, 2020, doi: 10.1109/5GWF49715.2020.9221122.

[7] M. Dr. Ir. Agus Wibowo, M.Kom, M.Si, *TELEKOMUNIKASI DIGITAL 5G*. Universitas Sains & Teknologi Komputer (Universitas STEKOM), 2021.

[8] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, "NFV and SDN-Key technology enablers for 5G networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2468–2478, 2017, doi: 10.1109/JSAC.2017.2760418.

[9] J. Krzywda, W. Tärneberg, P. O. Östberg, M. Kihl, and E. Elmroth, "Telco clouds: Modelling and simulation," *CLOSER 2015 - 5th Int. Conf. Cloud Comput. Serv. Sci. Proc.*, pp. 597–609, 2015, doi: 10.5220/0005494805970609.

[10] G. Jaro, A. Hilt, L. Nagy, M. A. Tundik, and J. Varga, "Evolution towards telco-cloud: Reflections on dimensioning, availability

and operability," *2019 42nd Int. Conf. Telecommun. Signal Process. TSP 2019*, pp. 1–8, 2019, doi: 10.1109/TSP.2019.8768807.

[11] A. Aijaz, "private_5G," no. December, pp. 136–145, 2020.