DDoS attacks prevention in cloud computing through Transport Control protocol TCP using Round-Trip-Time RTT

Thikra S Alibrahim [†], **Saloua Hendaoui** [††]

Department of Computer Sience, College of Computer and Information Sciences, Jouf University, KSA

Summary

One of the most essential foundations upon which big institutions rely in delivering cloud computing and hosting services, as well as other kinds of multiple digital services, is the security of infrastructures for digital and information services throughout the world. Distributed denial-of-service (DDoS) assaults are one of the most common types of threats to networks and data centers. Denial of service attacks of all types operates on the premise of flooding the target with a massive volume of requests and data until it reaches a size bigger than the target's energy, at which point it collapses or goes out of service. where it takes advantage of a flaw in the Transport Control Protocol's transmitting and receiving (3-way Handshake) (TCP). The current study's major focus is on an architecture that stops DDoS attacks assaults by producing code for DDoS attacks using a cloud controller and calculating Round-Tripe Time (RTT).

Key words:

DDoS attack ,Cloud Computing ,TCP protocol , Round-Trip-Time RTT.

1. Introduction

Large organizations are keen on providing cloud computing services. Cloud computing has changed the way information and communication technology (ICT) services are conceived, developed, deployed, scaled, maintained, reformed cloud computing is a set of computers that are connected to the Internet permanently and can be accessed anytime anywhere. The use of hardware and software to provide services to end-users across a network such as an internet is known as cloud computing. It consists of a collection of virtual machines that act as stand-ins for physical computers and deliver services like operating systems and applications [1].

The security of the infrastructure for digital and information services in the whole world is one of the most important pillars. With the expansion of the use of cloud computing in all areas, whether for individuals or private and governmental institutions, the security of these networks has become threatened. Clouds are attractive targets for attackers because of their elasticity, openness, and enormous big data stored.

Cloud models are based on common Internet protocols, they inherit the flaws in their enabling technology, such as virtualization. The cloud's flexibility and scalability also introduce new dangers, which can be exacerbated by the anonymity of the Internet [2].

Among these threats is the Distributed Denial of Services attacks (DDoS), which is known as the threat of distributed service blocking and works to block services of all kinds by sending packets of huge requests in succession so that the requests become greater than the capacity of the target until it collapses and goes out of service.

DDoS uses the Internet's inherent flaw, its open resource access approach, which, strangely, also happens to be its greatest strength.

Packet streams from various sources can be used for DDoS attacks [3].

Cloud DDOS attacks differ from ordinal DDOS attacks targeting normal systems. In the classic systems, DDOS occurs in the application layer, which targets server requests, i.e., computers or so-called zombies [4]unite to reach the server or website.

With the increase in attacks on the site, the volume of requests becomes excessive on the server and may cause it to stop. DDOS attacks on cloud computing reside on the network layer, mainly the Internet protocol (IP).

The second type is volumetric attacks and it is in the transport layer, mainly the Transport control protocol (TCP). The TCP¥IP controls the communication on the internet. Attackers can manipulate them which may cause weaknesses in the network.

The proposed research will be to protect cloud computing from DDOS attacks through TCP protocol, using cloud controller and Round-Tripe Time RTT.

The following is how the rest of the paper is organized: Section II includes an overview of cloud computing, while Section III a problem statement of the study, Section IV a study of the available literatures, Section V contains methodology, section VI as a results discussion, Finally paper's conclusion.

2. Cloud Computing

Cloud computing has gained widespread use in recent years and is now regarded as a significant technological advancement. Individuals and businesses have adapted it to provide faster and more convenient services.

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2022.22.1.38

The rise of cloud computing as a mainstream solution for massive data processing has transformed the digital world, allowing third-party service providers to deliver distantly and masse computing services[5].
The figure below explains the services and deployment of cloud computing.

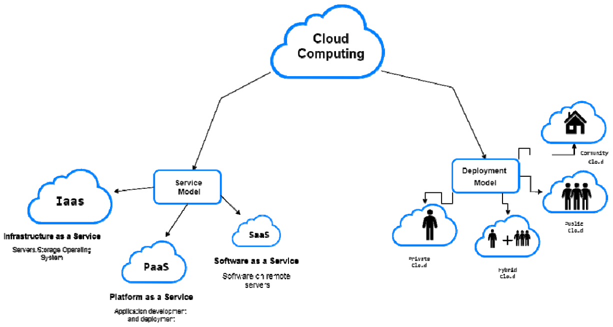


Fig. 1 Model of cloud computing service and deployment

2.1 Services of Cloud Computing

As shown in figure 1, cloud computing services can be categorized into three services:

i. SaaS (Software as a Service) Users can obtain software and other applications in the cloud using the SaaS approach. SaaS reduces the requirement for in-house applications, data storage, and maintenance.for the management of the application, Companies pay a fee to utilize the system. On a per-user basis, SaaS resources[6].

ii. PaaS (Platform as a Service) is a well-established approach in cloud computing for running applications without the hassle of managing hardware and software infrastructure on the user's end, such as Google App Engine, Windows Azure, and Force.com [7].

iii. IaaS (Infrastructure as a Service)The customer is given the power to supply processing, storage, networks, and other basic computing resources, allowing them to deploy and execute whatever program they choose[8]

2.2 Deployment of Cloud Computing:

Cloud computing deployment can be categorized into four main categories, as reported in figure 1:

i. Public Cloud: The majority of services are provided in a public setting, with users having access to a resource pool administered by a host business. This sort of setting will raise significant security concerns as a result of its presence.[9]

ii. Private Cloud: Private cloud infrastructure has many of the same advantages as public cloud infrastructure, but it is dedicated to a single enterprise. The cloud can be administered by the company itself or by a third party, and the infrastructure can be on-site or off-site. Private clouds provide you with more control over your cloud infrastructure, making them perfect for bigger businesses.[10]

iii. Community cloud: The community cloud is a cloud infrastructure that is shared among numerous communities or customers and can be hosted and managed internally or externally by a third party, or a hybrid of the two.[11]

iv. Hybrid cloud: A hybrid cloud combines two or more types of clouds (for example, a public-private cloud). This sort of deployment architecture offers great scalability and flexibility and a variety of data distribution possibilities because it reflects the characteristics of the associated clouds. A hybrid cloud is controlled from a central location [12].

3. Problem statement

DDoS attacks are one of the most common network threats, to flood the target with a large number of requests and data until it reaches a greater size. He falls or retires from his position of authority. DDoS attacks may be classified into three types:

i. Volume-based attacks:
User Data gram Protocol (UDP) and Internet Control Message Protocol (ICMP) flood assaults are examples of volume-based attacks. The attacker's goal in this assault is to saturate the bandwidth of the victim's side. The number of data or packets sent per second is referred to as bandwidth. As a result, the attacker's bandwidth must be greater than the victims. Bits per second is the unit of measurement for bandwidth.[13]

ii. Protocol-based Attack:
This type of attack tries to take advantage of network protocol flaws and devour the connection state tables that some network devices create[14], TCP and UDP protocols are exploited.

iii. Application Layer attacks:
Vulnerabilities in application layer protocols like Hypertext Transfer Protocol (HTTP) and Secure Sockets Protocol (SSL) are exploited.[14].

3.1 DDoS attacks for TCP

TCP is one of the most important network protocols, It is used to control data transmission over the network. The TCP protocol enables reliable communications for applications and services where datagrams are delivered in sequence, without mistakes, and duplication as long as there is a link-layer connection between two communicating endpoints. It ensures that flow control technologies like the sliding window protocol and adaptive re-transmission techniques are used to offer these services [15].

TCP works in a three-way handshake. We define the following scenario for TCP communication.

1) Device A sends SYN to devise D.
2) After reception of the SYN message by device D, it responds by SYN-ACK message.
3) When device A receives the SYN-ACK, it answers device D and sends the last packet from ACK

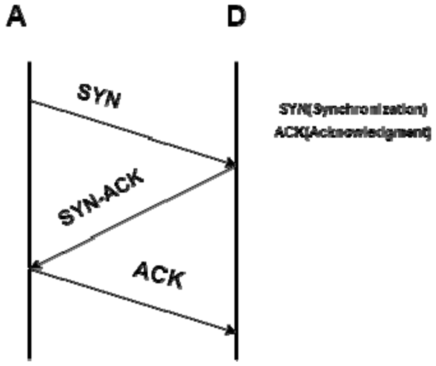


Fig 2 :TCP (3-way Handshake)

Attackers take advantage of the TCP protocol to respond to the request, where the hacker sends SYN in large quantities so that it cannot be answered and goes out of service.

3.2 SYN Flood

This attack makes use of a flaw in TCP, particularly in the "three-way handshake" process. When a device wants to communicate with another device in the network, it sends a packet of type (SYN) to the target, and the target responds with a packet of type (SYN / ACK) to let the device know that it is ready to receive data, so the device sends back a packet of type (ACK) to begin transferring data, and this is done in every packet sent between two devices in the network. It is of the type (SYN / ACK) and floods it with requests until it shuts down since it can no longer handle receiving them.

4. Literature Review

In [16] The authors provide a patented DD0S attack protection solution that reduces the vulnerability of the service. PINGIN was used to transmit 6500 packets for downgrade and disable testing, and Nmap was utilized to search for vulnerabilities in the target site port to test this technique. The first stage includes these two steps. The detection phase, which uses Wireshark to identify every incoming packet, is followed by the classification phase, which uses Random Forest and Naive Byes. When comparing the two, it is discovered that Naive Byes is superior in terms of prediction rating since the average mean of real packets is 0.982, but the malicious one is about 0.01 and functions in the same way.

P(b|c) = p(c|b) p (b / p(c) Where, P(c|b) is the likelihood P(b) = class prior probability. P(b) = prior probability of a class P(c) = previous chance predictor P(b|c) denotes the likelihood of anything happening in the future.

The discovered clusters as a consequence of naive Bayes are shown in this graph. This article hasn't been put into practice yet, and this approach hasn't been accepted as a viable solution to the problem.

The authors in [17]use NS-2 simulation with a specific network architecture to predict values for numerous distinct situations.

The network latency in attack scenario 1 is 22 milliseconds, attack scenario 2 is 2 milliseconds, and attack scenario 3 is 7 milliseconds. The assault cycle in all three attack situations is Ta = 2 s. The network delays dl=2ms in attack scenario 4, while the attack cycle is 5s.

They set nt bw = 100 Mbps, bn bw = 5 Mbps, bn dl = 6 ms, and the queue size at bottleneck B = 50 packets in this study. All simulations begin at 0 and conclude at 240, with the TCP stream beginning at 20 and ending at 240, with DDoS assaults beginning at 120 and ending at 220. (in units of seconds). They recorded TCP throughput in the time range of 160 to 180 times for each assault scenario.

They also used relative error as a means to determine the accuracy of this method and calculated it using the following law. This entire period is within the attack period (from time 120 to time 220) to consider TCP throughput in a steady-state rather than the average TCP throughput during the attack period.

$$\text{Relative error}=\frac{|Theortical\ Result-Expertmental\ Result|}{Expertmental\ Result}$$

The simulation results of this paper show that the relative errors are small, but this research needs more experiments to explore homogeneous and heterogeneous TCP flows.

In this paper[18] the author proposed an algorithm to redirect traffic to cloud servers and detect malicious movements using a firewall and a mitigation service was also used and suggested the presence of more than one server from several companies and synchronized with a database with firewalls on each server. All these algorithms are theoretical and have not been implemented Tested in the wall.

In this research[19], the researcher tested the three algorithms for machine learning, Support Vector Machine(SVM) Pattern recognition, spam filtering, and anomalous network intrusion detection all employ this basic machine learning approach, Random Forest is a machine-learning method that is both versatile and simple to use, as well as consistently producing excellent results and Naïve Bayes is a well-known probabilistic model that determines to categorize and learns to forecast the value of a new class by calculating probabilities for each class in the performance of WEKA tool. It was found that SVM is better in terms of accuracy, recall, and intrusion detection. But this technique was not tested to limit intrusion or prevent acceptance of consecutive requests.

In this paper[20], the author used GIDA consisting of Game Agent, Intrusion Detection System (IDS), Firewall, and Steering Module. TCP packet flow is analyzed by IDS Intrusion Detector and then BRO is used for Network Intrusion Detection (NIDS). The IP address and ports of the source and destination are extracted through the analysis. Execution time and duration and then the game agent uses this information to calculate the flow rates and return, However, this research applied simulations only theoretically and was not applied dynamically

In [21] paper, a solution is proposed to detect DDoS attacks by identifying static source IP (FSIA) and random source IP attacks (RSIA) and TCP-based real-time DDoS detection to distinguish between malicious and normal traffic in it. The results of this paper illustrate the different attack modes and distinguish traffic Benign network pass-through for major TCP attacks with high detection rates and low false alarm rates. However, there is a possibility of false alarm, meaning that it does not guarantee 100% safe operation

5. Methodology

The term "virtualization" refers to the creation of a virtual replica of something rather than a physical one. Virtualization is a technique for digitally reproducing a version of something actual in cloud computing[22]. In cloud computing, virtualization is the technology that is a virtual ecosystem of storage devices and server operating systems.

There are several types of rationalizations, categorized according to their used elements.

i. Server virtualization
   A virtual server allows several virtual machines to share a single physical server rather than a whole computer having its own[23].

ii. Storage virtualization
   Storage virtualization is the practice of aggregating physical storage from many network storage devices. Following the collection of several storage devices to the physical storage [24].

iii. Network virtualization
   is a way of combining network capacity by separating available bandwidth into channels, each of which is separate from the others and maybe allocated to or reassigned to a single server [25].

Although cloud computing is considered the big thing in the world of information technology, it involves many challenges. One of the biggest challenges and risks is the network restrictions such as low bandwidth and authentication and the security problem of cloud computing.

while the cloud may provide services to legitimate users, it can equally provide services to people with evil intent. A hacker can utilize a cloud and exploit network vulnerabilities to run a malicious program to achieve his goal, which might be a DDoS assault on the cloud.

As mentioned earlier, the attacker exploits the response to the request in the TCP as follows transmits the information bundles between the sender and the collector. The framework issues an SYN request, and the accepting framework responds with an ACK. The accepting framework's processing and memory resources request a transmission timeout for TCP SYN. TCP SYN assault in DDOS instructs the specialized to make TCP SYN requests to the casualty server.

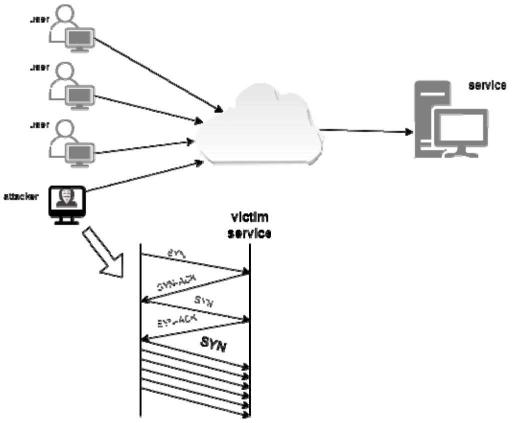


Fig 3 DDoS attack

DDoS attacks verify effective services by using multiple compromised computer systems for the attacker's traffic sources. It can include exploited devices, computers, and Internet-connected resources. The main attack system identifies and controls other vulnerable systems by infecting them with viruses or bypassing authentication controls by guessing the default traffic on a user's system or device. Authentication and low bandwidths are the most important cloud computing weaknesses and biggest security challenges for computing. A different approach was used in the authentication of cloud computing. The authentication differs in cloud computing according to cloud computing deployment, meaning that the authentication process in private computing is different from public computing.

The authentication procedure used in private cloud computing:

This authentication pattern is known as the trusted Identity Management (IDM) pattern. Google App Engine uses this type of user pattern to send its user credentials to the IDM component to encrypt user credentials, then send user credentials to an authenticator, who will decrypt user credentials and authenticate the user if authentication is successful via domain analyzer.

While user authentication is performed in public cloud computing:

When a user wants to access the public cloud, the user first sends their credentials to the external authenticator via Secure Sockets Layer (SSL) connection, then the authenticator checks the user's credentials in lightweight Directory Access Protocol (LDAP) servers, and if done, the user is granted access. After properly validating the user, it delivers valid attributes to IDM using the standard of security assertion markup language (SAMAL). The domain is then analyzed by IDM, and relevant services in the public cloud are granted access because the public cloud is primarily exposed to a bigger audience than the private-public cloud, the maintenance of the username password will require more space, and the number of authentication requests processed at the same time will also grow. As a result, an external authenticate is primarily responsible for public cloud authentication.

Since cloud computing is based on virtualization, controller cloud can be virtual to prevent the attacker's requests, we put a controller between the cloud and users in general. Attackers must be able to validate the user after the authentication procedure, notably in TCP connections, to breach authentication protocols and infringe on cloud computing services. The controller can calculating a Round-Tripe Time (RTT) otherwise known as round-trip delay (RTD) as a measure in milliseconds of the amount of time it takes to receive signal.

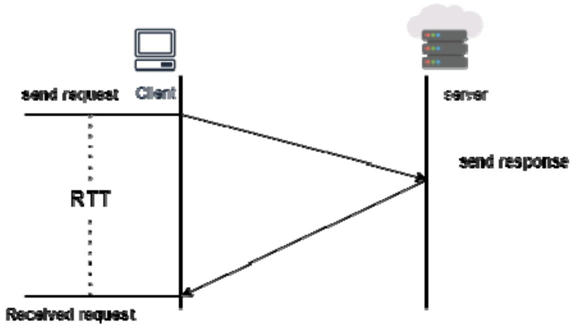


Fig 4 RTT

Where RTT calculated in TCP by
RTT= $\alpha * old\ RTT + (1 - \alpha) * new\ round$ Where α is {0 ≤ α < 1}

RTT is determined by the cloud controller, but it must be taken into account that:

1) If α is close to 0, then the value of sample RTT will be weighted heavily in the computation of the new Estimated RTT - the RTT estimate may vary too rapidly.
2) If α is close to 1, then the value of sample RTT will be weighted lightly in the computation of the new Estimated RTT - the RTT estimate vary slowly.
3) The recommended setting of α is some value from .07 to .09.

Figure below provide Cloud Controller:

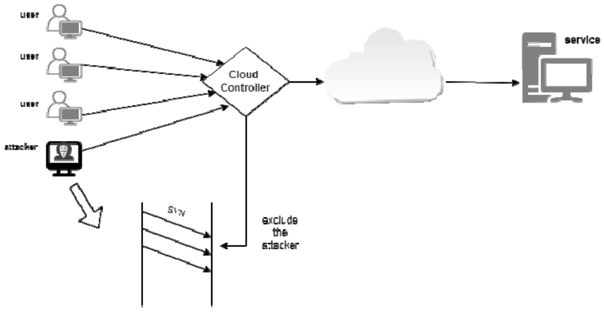


Fig 5 Cloud Controller

To prevent attackers from repeating these attacks and causing continuous system damage, a suspicions list must be established at the outset. If the user sends more than two packets and more than three times, the user is blocked because they are a DDoS attacker; if the user does not send more than two packets but is on the suspicious list, the user is trusted. The schema below shows that.

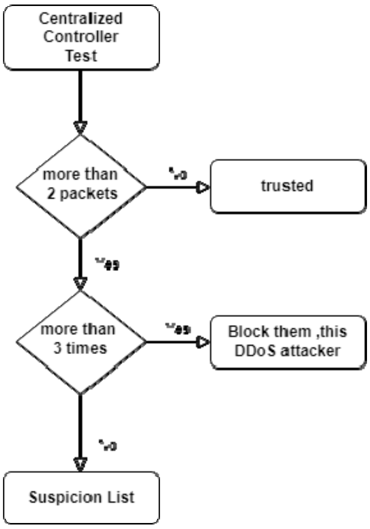
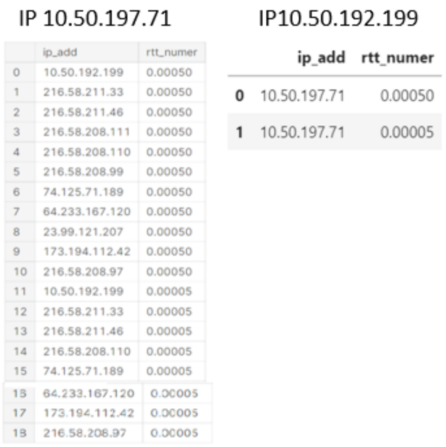


Fig 6 Centralized Controller

6. Results discussion

Using a dataset BOUN_TCP_Anon [26] we generated code using Python . choose two IP sources from the dataset with IP destinations. we determine two RTT and we experience the RTT for all destination.
The first IP source is 10.50.197.71 and second IP source is 10.50.192.199 we test with two RTT (0.0005, 0.00005).
First step specifies all attackers in two RTT as the table below:



IP 10.50.197.71

	ip_add	rtt_numer
0	10.50.192.199	0.00050
1	216.58.211.33	0.00050
2	216.58.211.46	0.00050
3	216.58.208.111	0.00050
4	216.58.208.110	0.00050
5	216.58.208.99	0.00050
6	74.125.71.189	0.00050
7	64.233.167.120	0.00050
8	23.99.121.207	0.00050
9	173.194.112.42	0.00050
10	216.58.208.97	0.00050
11	10.50.192.199	0.00005
12	216.58.211.33	0.00005
13	216.58.211.46	0.00005
14	216.58.208.110	0.00005
15	74.125.71.189	0.00005
16	64.233.167.120	0.00005
17	173.194.112.42	0.00005
18	216.58.208.97	0.00005

IP10.50.192.199

	ip_add	rtt_numer
0	10.50.197.71	0.00050
1	10.50.197.71	0.00005

Fig 8 Attackers IP

The flowcharts explains the number of attackers in both RTT

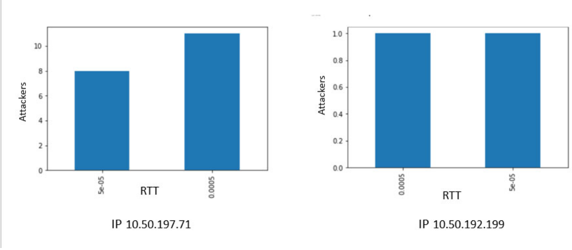


Fig 9 no. attackers with RTT

This flow diagram expound the average of attackers at both RTT as at 1 he is attacker at one RTT ,at 2 he becomes the attacker at both RTT.

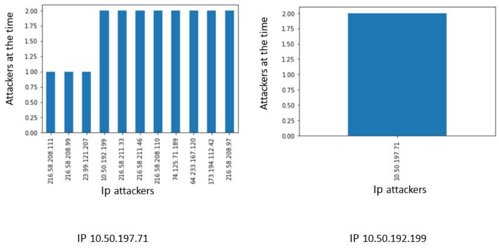


Fig 10 An average of attackers in RTT

7. Conclusion

with the increasing need for computing resources and applications, the need to secure these resources and applications and protect them from any attack, including a distributed denial of service attack, has increased, because this attack negatively affects both the service provider and the beneficiaries of cloud computing services and applications. Setting the cloud controller for the RTT account and choosing the appropriate RTT helps protect cloud computing resources and applications, especially as it is a centralized controller that determines whether this user is trust or attacker and blocked the attacker and identifies who the suspicious users are.

Acknowledgment

The authors would like to thank the Deanship of Graduate Studies at Jouf University for funding and supporting this research through the initiative of DGS, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.
.

References

1. Darwish, M., A. Ouda, and L.F. Capretz. Cloud-based DDoS attacks and defenses. in International Conference on Information Society (i-Society 2013). 2013. IEEE.
2. Carlin, A., M. Hammoudeh, and O. Aldabbas, Defence for distributed denial of service attacks in cloud computing. Procedia computer science, 2015. 73: p. 490-497.
3. Osanaiye, O.A., DDoS defence for service availability in cloud computing. 2016.
4. Gupta, B., R. Joshi, and M. Misra, Prediction of a number of zombies in a DDoS attack using a polynomial regression model. Journal of advances in information technology, 2011. 2(1): p. 57-62.
5. Dixit, S., Cloud Computing Security aspects: Threats, Countermeasures and Intrusion Detection using Support Vector Machine. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021. 12(10): p. 2271-2277.
6. Alouffi, B., et al., A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. IEEE Access, 2021. 9: p. 57792-57807.
7. Siddiqui, S.T., et al., Cloud-based e-learning: using cloud computing platform for effective e-learning, in Smart Innovations in Communication and Computational Sciences. 2019, Springer. p. 335-346.
8. Miyachi, C., What is “Cloud”? It is time to update the NIST definition? IEEE Cloud computing, 2018. 5(03): p. 6-11.
9. Alam, T., Cloud Computing and its role in Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 2021. 1: p. 108-115.
10. Attaran, M. and J. Woods, Cloud computing technology: improving small business performance using the Internet. Journal of Small Business & Entrepreneurship, 2019. 31(6): p. 495-519.
11. Ali, M.B., T. Wood-Harper, and R. Ramlogan, A Framework Strategy to Overcome Trust Issues on Cloud Computing Adoption in Higher Education, in Modern Principles, Practices, and Algorithms for Cloud Security. 2020, IGI Global. p. 162-183.
12. Alhenaki, L., et al. A survey on the security of cloud computing. in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). 2019. IEEE.
13. Harshita, H., Detection, and prevention of ICMP flood DDOS attack. International Journal of New Technology and Research, 2017. 3(3): p. 263333.
14. Balarezo, J.F., et al., A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. Engineering Science and Technology, an International Journal, 2021.
15. Schuba, C.L., et al. Analysis of a denial of service attack on TCP. in Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097). 1997. IEEE.
16. Amjad, A., et al., Detection and mitigation of DDoS attack in cloud computing using a machine learning algorithm. EAI Endorsed Transactions on Scalable Information Systems, 2019. 6(26).
17. Kieu, M.V. and T.T. Nguyen. A way to estimate TCP throughput under low-rate DDoS attacks: one TCP flow. in 2020 RIVF International Conference on Computing and Communication Technologies (RIVF). 2020. IEEE.
18. Sahu, S.K. and R. Khare, DDOS Attacks & Mitigation Techniques in Cloud Computing Environments. Gedrag Organ. Rev, 2020. 33(2): p. 2426-2435.
19. Wani, A.R., et al. Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques. in 2019 Amity International conference on artificial intelligence (AICAI). 2019. IEEE.
20. Bedi, H.S., S. Roy, and S. Shiva. Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows. in 2011 IEEE symposium on computational intelligence in cyber security (CICS). 2011. IEEE.
21. Jiao, J., et al. Detecting TCP-based DDoS attacks in Baidu cloud computing data centers. in 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). 2017. IEEE.
22. Shukur, H., et al., Cloud computing virtualization of resources allocation for distributed systems. Journal of Applied Science and Technology Trends, 2020. 1(3): p. 98-105.
23. Atiewi, S., A. Abuhussein, and M.A. Saleh. Impact of Virtualization on Cloud Computing Energy Consumption: Empirical Study. in Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control. 2018.
24. Malik, M.I., S.H. Wani, and A. Rashid, CLOUD COMPUTING-TECHNOLOGIES. International Journal of Advanced Research in Computer Science, 2018. 9(2).
25. Kumar, R. and S. Charu, An importance of using virtualization technology in cloud computing. Global Journal of Computers & Technology, 2015. 1(2).
26. Erhan, Derya (2020), “Boğaziçi University Distributed Denial of Service (BOUN DDoS) Dataset”, Mendeley Data, V1, doi: 10.17632/mfnn9bh42m.1

Thikra Alibrahim: Master student in jouf university received the B.E.. degrees, from jouf Univ in 2021.

Saloua Hendaoui received the B.E. and M.E. degrees, from tunis Univ. in 2011 and 2009, respectively. She received the Dr.. degree from Cartage Univ. in 2017. Working as a assistant professor (from 2018) in the Dept. of computer Science Jouf University.