# A Hybrid Deep Learning and Blockchain Framework for Mitigating Distributed Denial-of-Service Attacks

Shadman Skaib Sadvi , Wong Eugene , Arvin Angkasa , Tan Teck Sheng , Sai Wen Xiang , Noor Ul Amin *

Posted Date: 5 December 2025

doi: 10.20944/preprints202512.0440.v1

Keywords: Distributed Denial-of-Service (DDoS); cybersecurity; network security; traffic analysis; deep learning; convolutional neural networks (CNN); blockchain; adaptive filtering; dynamic traffic analysis; intrusion detection systems (IDS); network defense; anomaly detection; cyberattack mitigation; AI in cybersecurity

*Article*

# A Hybrid Deep Learning and Blockchain Framework for Mitigating Distributed Denial-of-Service Attacks

**Shadman Skaib Sadvi, Wong Eugene, Arvin Angkasa, Tan Teck Sheng, Sai Wen Xiang and Noor Ul Amin ***

Taylor's University

* Correspondence: nooraminnawab@gmail.com

**Abstract**

This report mainly focuses on researching, identifying and analysing popular cyber attacks affecting individuals and organisations worldwide. Our group is needed to research about the selected cyberattack, Distributed Denial-of-Service ( DDoS) background, recent related cyberattack cases, and reasons for getting attacked and think about the series of countermeasures to enhance the security measurement and prevent it from happening again. After thorough research, our group found that DDoS attack is one of the most unpreventable because it exploits weaknesses of the network topologies and standard protocols which makes it very difficult to prevent, hackers just have to overwhelm the system server. Thus, we think of implementing a "dynamic network traffic analysis and adaptive filtering system" and "blockchain-based traffic authentication" to enhance the security measures. Both systems are effective in filtering flooded traffic packages sent by non-human devices from overwhelming the server's resources.

**Keywords:** Distributed Denial-of-Service (DDoS); cybersecurity; network security; traffic analysis; deep learning; convolutional neural networks (CNN); blockchain; adaptive filtering; dynamic traffic analysis; intrusion detection systems (IDS); network defense; anomaly detection; cyberattack mitigation; AI in cybersecurity

---

## 1.0. Background

### *1.1. Background of DDOS*

A distributed Denial-of-Service(DDOS) attack aims to play havoc with services by trying to restrict access to the machine rather than undermining the service directly. DDOS is the kind of attack that renders a network inaccessible by users by attacking either the network's bandwidth or its connectivity. These attacks accomplish their objective by inundating their victim with packets that overwhelm the victim's network or other processing capacity, thereby rejecting access for their regular clients.

### *1.2. History*

DDoS ironically started with a 13 year-old student at University of Illinois High School. His name was David Dennis. David carried out an experiment by writing a program that sent a problematic command to a terminal called PLATO which managed to shutdown 31 terminals of PLATO at once. This small experiment was carried out under supervision so no harm was caused to any hardware or software. However, this small experiment was the start of an ongoing threat to everyday cybersecurity personnel.

With the development of IRC(Internet Chat Relay) booming in the 90's, this phenomenon created a pathway for simple bandwidth-based DDoS attacks in order to gain access to admin control of a chat room. Essentially with IRC, if you're logged off, the user will lose access to admin rights and will not be able to control the chat room. Although such DDoS attacks were run-of-the-mill for

 doi:10.20944/preprints202512.0440.v1



cybersecurity personnel at this day and age to solve, it is nowhere near what companies are facing today when it comes to DDoS attacks, especially big-name companies such as Apple, Sony, Samsung, and many more.

How did DDoS become a weapon you may ask? The earliest victim of a major DDoS attack was a New York-based Internet service provider named Panix in 1996. The hacker used a SYN flood to overwhelm Panix with fake "synchronise" packets from a spoofed IP address. The packets halted the company's ability to process legitimate requests. This forced Panix to take 36 hours to recover from this attack which was very prompt. However, this incident marked a significant milestone in the history of DDOS attacks and thrust DDoS into the limelight once again.

Three years later, DDoS was seen again with its attacks. This time around, the University of Minnesota was the victim. The University was faced by severe disruption when a hacker employed a massive UDP flood, using a tool called Trinoo. Trinoo is a comprehensive tool that is used to carry out DDoS attacks and allows a hacker to create, prepare and implement a DDoS attack. This attack completely crippled the university's internal network for over 48 hours, gaining significant public attention in the process. This event significantly highlighted the growing threat that DDoS is capable of in the computer world.

Among the most notorious DDoS hackers is a well-known hacker called Michael "Mafiaboy" Calce. In 2000, while Michael was still a teenager, he formed a DDoS attack on major corporations including CNN, Yahoo, Amazon, Dell, eBay, and FIFA. Michael utilized a tool called TFN2, which compiles previously infected computers to generate a flood of fake traffic to the network. On top of that, Michael managed to bypass standard network communication protocols by tampering with the encryption.

Mafiaboy really set the tone for other hackers by demonstrating the devastating potential of DDoS strategies while inspiring others in the hacking world to do the same. This caused hackers around the world to revolutionise DDoS techniques and methods that increase the efficiency of the attacks to cause them to be more vicious. Subsequently, numerous large-scale attacks were carried out by hackers, who targeted corporations for political incentives or extortion. These incidents were just the beginning of a growing and complex issue in cybersecurity.

*1.3. Architecture*

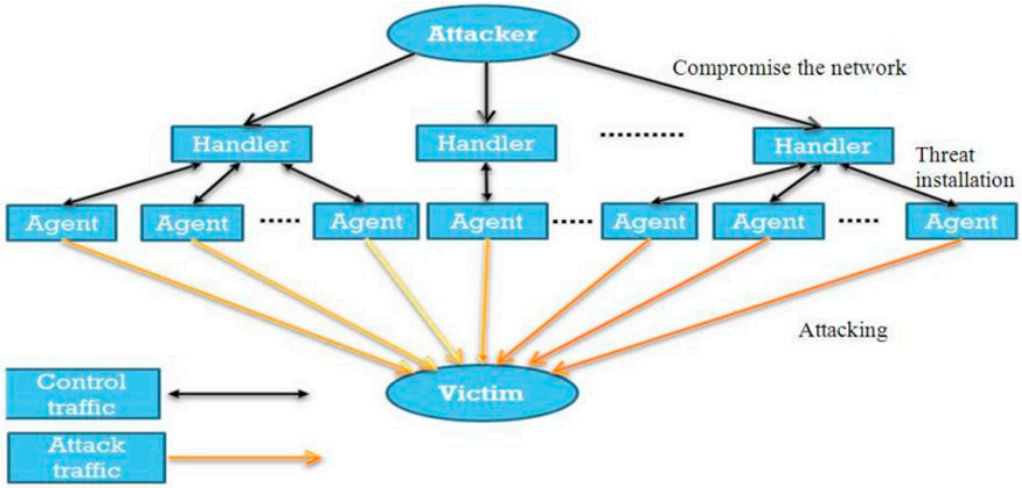


**Figure 1.** Architecture of distributed denial of service (ddos) attack | download scientific diagrams. (n.d.). https://www.researchgate.net/figure/Architecture-of-Distributed-Denial-of-Service-DD oS-attack_fig1_265053091.

Based on the image above we are able to deduce how a DDoS attack occurs. Firstly, the attacker is able to gain access to the agents through the handlers. The attacker chooses the handlers with security vulnerabilities first and gains access rights to the handlers. In order to carry out a successful

 doi:10.20944/preprints202512.0440.v1



attack, the attacker chooses as many network handlers and agents as possible. This allows the attacker to install vulnerabilities in a specific time using ICMP (Internet Control Message Protocol). ICMP is often used during this phase since it is able to help identify active hosts and their network configurations, making it easier to find vulnerabilities in the system.

In order for the attacker not to be tracked, the agents and handlers are located outside the victim's and attackers network. This geographic distribution helps obscure the origin of the attack and makes mitigation more challenging for the victim. Once the agents are compromised, agents are instructed to send a large volume of useless packets to the victim simultaneously. This is the core of the DDoS attack. The attack traffic can vary including TCP(Transmission Control Protocol), UDP (User Datagram Protocol), and ICMP (Internet Control Message Protocol). Each type of packet serves a different purpose and can be used to overwhelm different aspects of the target's network.

Moving on to the victim's point of view. Once the victim's network is overwhelmed by a massive influx of malicious traffic, this leads to denial of service since the service is unable to determine whether legitimate users are trying to access the service. The primary goal of the attack is to shut down the service availability of the victim, causing significant disruption and potential financial loss to the victim[51–53].

Most attackers use IP spoofing to make it harder to trace the attack back to its origin. IP spoofing works by making the attack traffic appear as though it's coming from multiple different sources[54–57]. On the other hand, random source ports are used to complicate detection and mitigation efforts[58–61]. The randomness in random source ports allows the attacker to evade security measures like port-based filtering[62–64].

## 2.0. Discussion on Security Issues

### *2.1. Scenario 1: AWS DDoS Attack in 2020*

In February of 2020, Amazon Web Services (AWS) was attacked by an enormous DDoS attack. Intruder using Connectionless Lightweight Directory Access Protocol (CLDAP) which is a technique of using third party CLDAP server to enlarge the volume of traffic on AWS server. Although AWS Shield mitigated this gigantic DDoS attack which peaked at 2.3Tbps, it still caused the staff in AWS Shield to experience three days of "elevated threat". To mitigate the DDoS attack, we must understand and investigate what technique the intruder used and how it works first.

*Connectionless Lightweight Directory Access Protocol (CLDAP)*

CLDAP is a variant of Lightweight Directory Access Protocol (LDAP) which is used among various devices to access directory services such as active directory. Unlike LDAP which usually served over TCP, CLDAP avoids protocol overhead such as handshaking on establishing communication between devices to enhance the performance. To simplify it, CLDAP is a UDP version of LDAP. Users can obtain a large response by sending a small request. This significant attribute provides intruders a tool to amplify the volume of the attacks to overwhelm the capacity of the server. According to the studies, intruders can amplify the data that is sent to the victim's IP address up to an astounding 56-70 times. This means victims would have to handle 70 bytes of data if the intruders send only a bytes of request.

At the beginning, the attacker will first scan for a server that is able to respond to CLDAP requests with automated tools. After discovering these servers, intruders will send CLDAP requests to all these servers with a spoofed IP address, which is the victim's IP address. These servers will send back a larger volume of data than it received to the "victim's request" which was originally sent by the intruders. In this case, AWS server acted as the victim, which intruders send a lot of CLDAP requests with AWS server IP address to try to flood its server.

 doi:10.20944/preprints202512.0440.v1



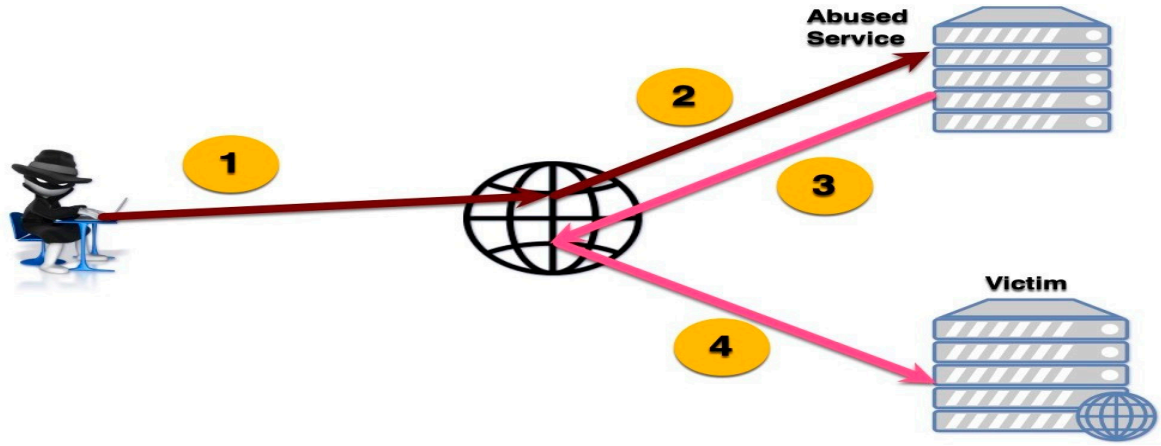


**Figure 2.** DDoS Attack by using CLDAP with spoofed IP address by Tom Ozlak (2022) Available at: https://www.spiceworks.com/it-security/cyber-risk-management/articles/defending-against-cl dap-reflection-attacks/.

To achieve this massive DDoS attack, some studies believe that the intruders use a combination of CLDAP and botnet techniques to achieve such a large attack. By contracting with the botnet service provider or spreading the malware to gain control from other devices on the network, intruders can get a large number of devices. Each of the infected devices send the request to all the vulnerable servers with spoofed IP addresses causing such a large volume of traffic directed to the AWS server.

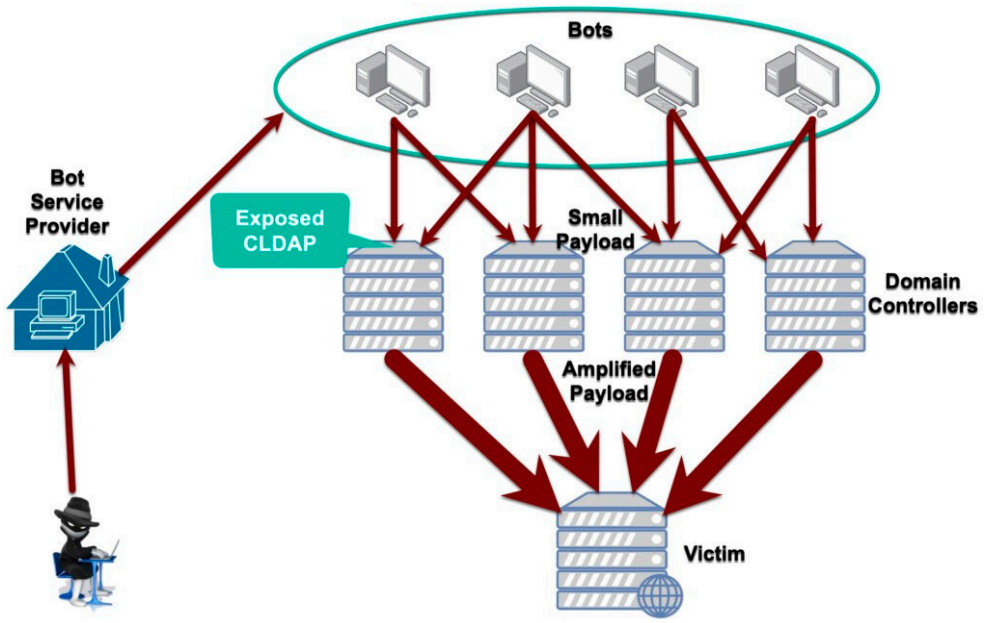


**Figure 3.** DDoS Attack by using botnets and CLDAP with spoofed IP address by Tom Ozlak (2022)Available at: https://www.spiceworks.com/it-security/cyber-risk-management/articles/defending-against-cl dap-reflection-attacks/.

In conclusion, the intruders in this case misuse the vulnerable characteristics of CLDAP to launch amplification attacks to AWS servers causing the company to fall into an emergency situation for a few days[65–67].

The scenario have brought us a some important message in AWS server security issues:

The purpose of CLDAP is to speed up the performance of accessing directory services over the networks. In the scenario, the intruders use the characteristics of this protocol to enhance its DDoS attack. Since the amount of data of response is always larger than the request, intruders use this

 doi:10.20944/preprints202512.0440.v1



mechanism to amplify the amount of data to try to crash the server. This kind of amplification attack also attracts intruders to launch an attack because it doesn't require complex knowledge and tools to launch it.

In the scenario, intruders don't launch a DDoS attack by using devices directly but using third-party servers to send an amplified amount of data to the AWS server. This not just harms the availability of AWS servers but also occupies the computing resources of these third party servers. In addition, it is hard to detect and defend against such attacks since the intruders use legitimate servers and legitimate traffic to send the massive data.

Although AWS Shield has successfully mitigated this massive attack, and defended their client from this attack, the attack still caused three days of disruption to the staff. The strategies of detection and mitigating should be improved in future to handle more complex and larger attacks in the future.

These security issues must be quickly solved by AWS rapidly to ensure the availability of the server which is a part of CIA is working well. If those issues didn't get addressed properly, some potential security threats would threaten AWS.

AWS might break its largest DDoS attack record again if they didn't address the issues well. Intruders launch DDoS Attack via third party servers which respond to the CLDAP requests, AWS cannot identify the real attacker since most of these servers are ordinary and have no clear sign. In addition, intruders usually use botnets to launch DDoS attacks also harming the computing resources of the devices. These third party servers will be abused by the intruders again if the owner of the servers didn't realise and address the bugs properly.

AWS Shield provides advanced protection against DDoS which is hard for intruders to break the availability. It requires a high level of skills in all aspects of cybersecurity to launch a gigantic DDoS attack that causes AWS Shield to fall into emergency days. Thus, intruders in the scenario most probably an expert or a group of experts in cybersecurity. Those intruders have the capabilities to launch more sophisticated attacks in future which threaten the service provider such as AWS and their client.

### *2.2. Scenario 2: Microsoft Azure (2021)*

Microsoft Azure, one of the world's largest cloud computing platforms in the world had encountered an unprecedented cyberattack, it is a Distributed Denial-of-Service (DDoS) attack that happened in the second half of 2021. The DDoS attack aimed to attack the organisation's servers by occupying their servers' resources causing the whole system to be malfunctional for both clients and admin. The rise of DDoS attacks had been a significant cyber threat in late 2021, by sending trillions of service requests forcing servers to be overloaded and eventually stopped.

What Azure specifically was dealing with is a reflection attack and amplification attack. A reflection attack is when the attacker sends a request to the third-party server with the source IP address spoofed to become the target's IP address. Then the server sends the response to the target, which will overwhelm it with responses.

 doi:10.20944/preprints202512.0440.v1



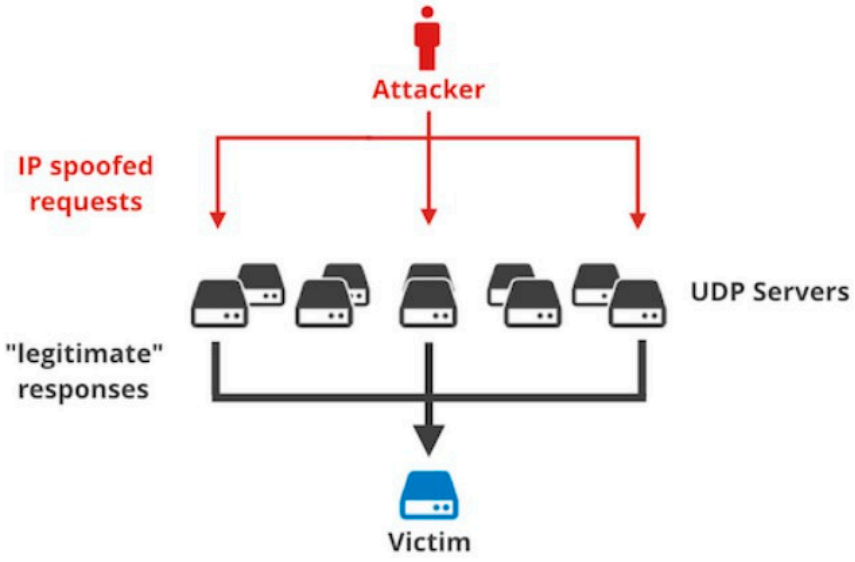


**Figure 4.** Reflection Attack Marek Majkowski (2017) Available at: https://blog.cloudflare.com/reflections-on-reflections.

An amplification attack is also used to work with the reflection attack used, an amplification attack is an attack technique which exploits protocols that generate larger responses than the initial request, for example, the attacker uses a small request that will trigger a larger response from the server and thus it will amplify the attack's traffic volume.

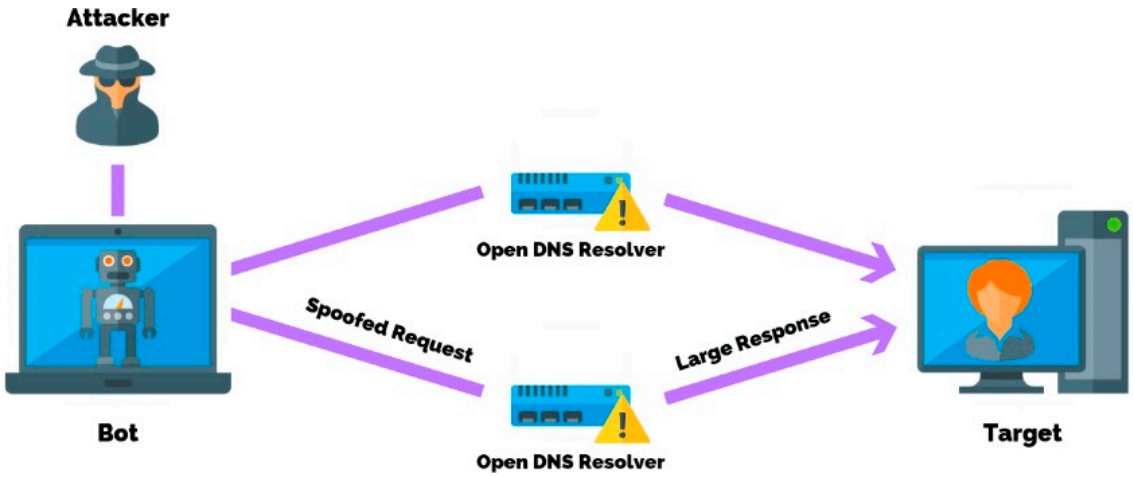


**Figure 5.** DNS Attack using botnet Jason Firch (n.d.) Available at: https://purplesec.us/prevent-dns-amplification-attack/.

First wave: August 2021

The first attack peaked at 2.4 Terabits per second (Tbps) which was experienced by an Azure client in Europe. The technique implemented by the attacker is the **UDP reflection**, this technique exploits the User Datagram Protocol (UDP) amplifying traffic by bouncing off multiple intermediate servers originating from approximately seventy thousand countries in the Asia-Pacific Regions and the United States (Sharma, 2021).

The second wave (Largest): November 2021

The second attack peaked at 3.47 Terabits per second (Tbps), the attack was targeting Azure customers in Asia. This attack was recorded to involve 340 million packets per second originating from over ten thousand nations all across the globe like the United States, Iran, India, Vietnam, etc (Azure, 2023).

The security issue identify: ***Exploitation of UDP port***

 doi:10.20944/preprints202512.0440.v1



**UDP reflection** is the primary security concern raised in the aforementioned examples. UDP reflection operates by having the attacker send a request to an accessible server, such as the DNS server, spoofing the target's IP address. The accessible server will then use the three-way handshake protocol to respond to the target server as usual. Subsequently, the assailant will enhance the efficacy of the attack by concurrently initiating many server requests with a forged IP address. Internal reflection eventually happens on servers, overloading the system and resulting in a denial of service.

The **potential security threat** that might occur if the issue is not addressed correctly is **data breaching**. Data breaching will be one of the most common second attacks on DDoS because the attacker has completely taken control of the server, they will be able to change the privilege and steal the organisation or client's sensitive information illegally. Furthermore, attackers can launch **ransomware** easily when there is a denial of service to get funds from victims after freezing their servers.

Phishing could also be a potential security threat for Microsoft Azure. Phishing is basically using the stolen data from the previous attack to target the clients themselves, this will create a very bad reputation for Microsoft Azure as because of them getting the attack, the clients are also affected as their data have also been breached and used against them.

## 3.0. Discussion on Security Countermeasures

*3.1. Security Countermeasures*

3.1.1. Blackhole Routing

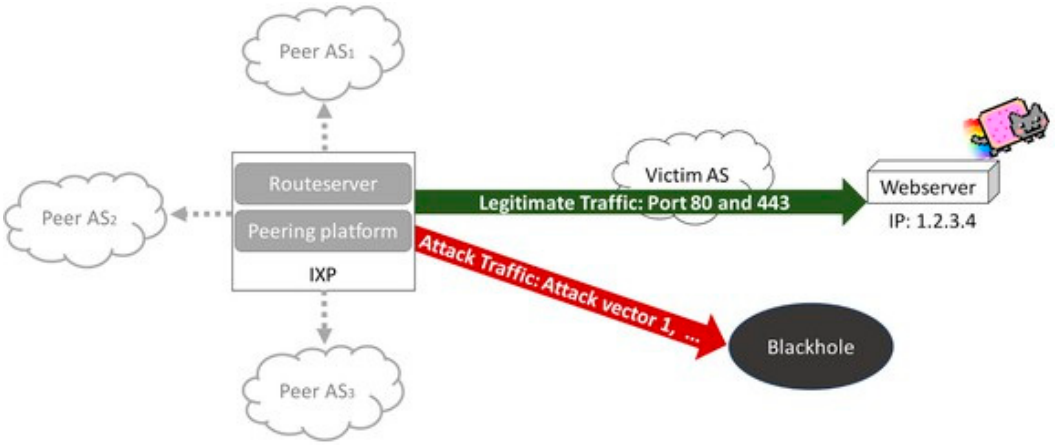


**Figure 6.** Blackhole Routing.

Blackhole routing is one of the techniques to counter the Distributed Denial of Service (DDoS) attack. This technique will route all the unwanted and harmful traffic into a blackhole to prevent it from reaching the destination. This technique is not the best choice but it is good for organisations that don't have any way to block an attack, as this is widely available and easy to use. This blackhole routing not only can reduce the DDos attack effectively, but it can also improve the overall network performance by reducing network conjestion. However, blackhole routing will block all the traffic to a specific IP address regardless good or bad therefore we must use this technique carefully to prevent downtime. So there are a few ways to implement blackholing which is BGP blackholing, and blocklists for spam filtering. Border Gateway Protocol (BGP) blackholing is used to reroute the traffic into the blackhole to prevent the network from causing harm. But this BGP blackholing requires BGP peering so that it can control the flow of the traffic on their network by the network administrators. Compared with blocklists for spam filtering, both are same effective but it serves different purposes, as the Blocklist only can and is effective if implemented at the email filtering, it does not handle any network wide attack like the BGP blackholing.

 doi:10.20944/preprints202512.0440.v1



3.1.2. Filtering and Limiting

Both Filtering and Limiting are the mechanisms that are used to implement security countermeasures. For these two mechanisms to work, it requires a detection mechanism to analyse the incoming traffic and identify the malicious pattern and provide the information for the filtering and rate limiting system. One of the detection mechanisms to monitor, analyse and identify the malicious activities in the traffic, is to install an intelligent router within the ISP network. The responsibility of this router is to authenticate the request by issuing a puzzle to the client and sending it back to the user if the request is suspicious. As this Puzzle can be easily solved by humans but difficult for bots, failing to solve the puzzle will be confirmed as an attack bot.

This detection mechanism can make the filtering mechanism more effective as the filtering mechanism is designed to analyse the incoming traffic and block the packets that match the patterns of the traffic attack, the detection mechanism not only helps to increase accuracy by distinguishing legitimate users and bots but it also reduces the false positive.

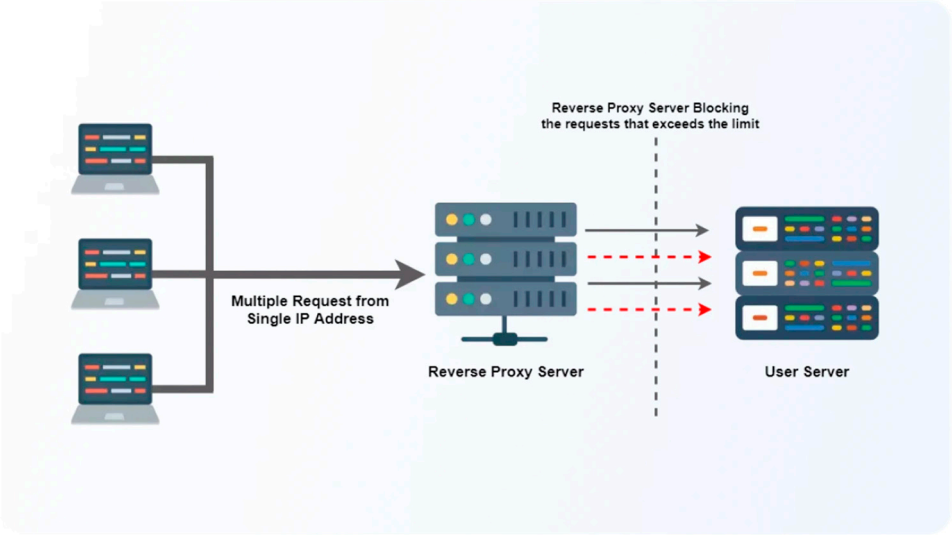


**Figure 7.** Rate Limiting Mechanism.

For the Rate limiting mechanism, it is used to control the rate of request per min from a same IP address to prevent the system overwhelm. This mechanism is recommended when the detection system generates too many false positives or when it is hard to determine which IP addresses are malicious attacks, as this mechanism can reduce the damage without blocking the entire traffic.

3.1.2.1. Pushback high-bandwidth aggregates

Pushback high-bandwidth aggregates is a method which is part of Aggregate-base Congestion Control (ACC) that is used in network management to control and manage the high-bandwidth traffic that might cause network congestion. While this method is different than the filtering mechanism, as the filtering mechanism block the suspicious traffic by using the pattern that match with the known attack pattern, but the Pushback high-bandwidth aggregates is different as the ACC first detect and identify the congestion such as high packet loss rate, when ACC detected a high packet loss rates, the router will use the pushback mechanism to communicate with the upstream router and adjusting the flow rate on the identified high-bandwidth flow to prevent and reduce network congestion.

3.1.3. Stateless Internet Flow Filter (SIFF)

Stateless Internet Flow Filter is a mechanism that is designed to prevent and counter DDoS attacks by managing and controlling the flow of the traffic using the capability tokens. The Capability

 doi:10.20944/preprints202512.0440.v1



token will authenticate and authorise packets, allowing the Stateless Internet flow filter to distinguish the privilege and unprivileged packets. The router will allow packets that have valid capability tokens which are privileged packets to pass through the network and the unprivileged one will be filtered out or given lower priority. The capability token will be provided to the trusted client in the beginning of the handshake, so that the SIFF can prioritise the privileged packets over the unprivileged one to reduce the impact of DDoS attack. This capability tokens require regular updates from the server to remain valid as the token is time limited to prevent misuses. To effectively filter out the unwanted traffic, this system have an additional layer of security which during the handshake layer the involving Explorer packets and the subsequent verification of Data packets will ensure only the client who successfully complete the handshake are able to send the privilege traffic to verify the legitimacy of the clients

### *3.2. Proposed Countermeasures*

#### 3.2.1. Dynamic Traffic Analysis and Adaptive Filtering

Traditional traffic analysis works based on a predefined set of rules which can be rendered obsolete within a short period as attackers adapt their strategy. We can therefore introduce dynamic traffic analysis and adaptive filtering based on the analytical results without human intervention. This can be achieved by adapting a Convolutional Neural Network into the defence system.

To adapt a CNN we need to feed data about incoming traffic into the network. We can use the ip packet headers and process them to produce 2d formatted data which can be fed into the model. Feature extraction can be done on the data to identify attack patterns and anomalies in the data which can indicate malicious activity. Feature extraction on cnn is done by two methods which are convolutional layers and pooling layers. Convolutional layers apply different filters on the data which helps recognize patterns in the data, such as spikes in packet size or abnormal timing intervals. Pooling layers reduce data dimensionality helping summarise the presence of features in the input. This reduces the computational overhead by focusing on relevant patterns.

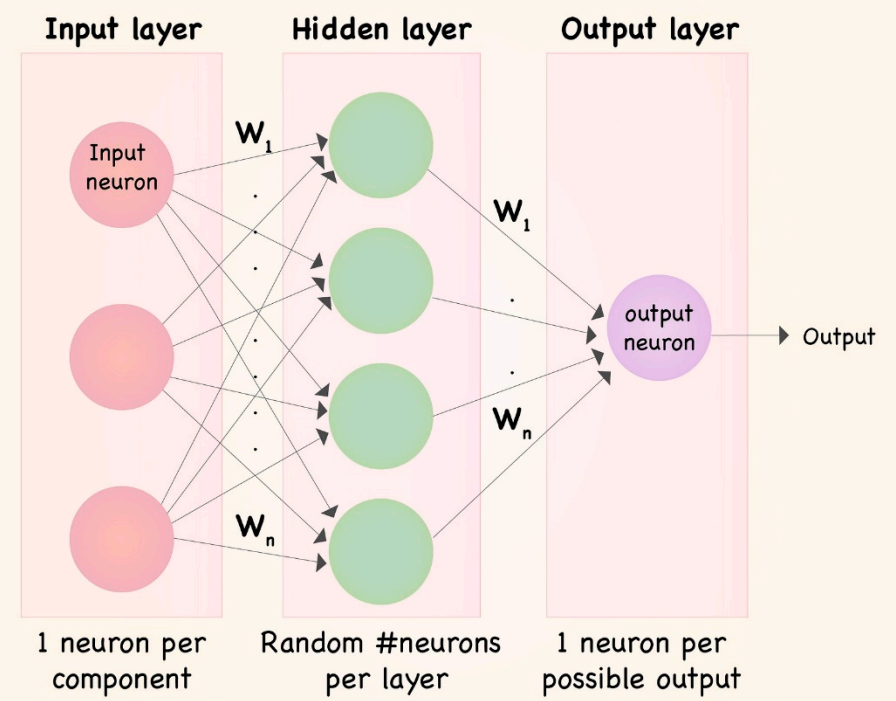


**Figure 8.** Simple Neural Network.

The CNN can be trained in either two ways. Hard scoring traffic as malicious or scoring them as a probability. Cnn as a classifier can classify traffic as normal, DDoS traffic or other intrusion activities

 doi:10.20944/preprints202512.0440.v1



based on the training provided. In such cases the cnn flags traffic as malicious either malicious or not. The other would be the scoring approach which scores the input traffic, where the score indicates the likelihood of traffic being malicious.

Once flagged by the CNN the firewall or setup defence system can adapt its rules to block or limit malicious traffic, all the while without any obstruction to regular traffic, thus adaptively filtering out malicious traffic without the pattern being defined previously. This type of filtering can be leveraged for real time traffic filtering and as a feedback looping/ recursion. While the cnn output is primarily used to filter traffic in real time, the logs produced can be used to further train the cnn. By further training the CNN on the traffic logs and patterns we can create a sort of cyclic recursion of prevention and feedback. Thus with each prevention the can effectively gets better and more robust at handling traffic.

#### 3.2.2. Blockchain-based traffic authentication

Another approach which can be used to prevent DDoS is by leveraging the blockchain based verification for incoming traffic. Blockchains work on the principle of immutable data signature hashing to prevent spoofing or editing of data. We can apply this principle to incoming traffic.

Each packet is hashed by network cards using a secure hashing algorithm (SHA256, etc) which produces a unique and identifiable hash. To be noted that only certain elements in the header are hashed (ip, timing intervals, etc). This hash can then be broadcasted to the rest of the chain which can then validate the hash or reject based on certain set of rules. Once accepted the hash which now acts as a fingerprint of the traffic packet and is added to the block ensuring that it is immutable and verifiable.

Upon arrival the packets are verified against the stored hash (re-hashed). If the hash matches the traffic is considered normal traffic. Mismatched hashes can be an indicator of spoofing or tampering. Indicating malicious activity.

Flagged traffic is flagged, logged and restricted and prevented from overwhelming the system.

## 4.0. Conclusion

In summary, the Distributed Denial of Service (DDoS) attack is considered one of the significant cyberattacks that everyone must be aware of because it is tedious to handle post-attack recovery and carry out the forensics process. Over the years, DDoS attacks has successfully compromised big companies such as GitHub in 2016, Sony PlayStation Network in 2014, BBC in 2015, OVH and Dyn in 2016. Two countermeasures that our group figured out were able to effectively filter out botnets from flooding into the server because of the implementation of cutting-edge technologies, Deep learning and blockchain. Deep Learning technology allows the system to recognise and classify normal, abnormal, and DDoS traffic through neural networks. In contrast, blockchain uses the hashing algorithm and chain to ensure it is not immutable. Nevertheless, there is no perfect countermeasure to completely block this issue from happening because technology is evolving drastically every day, and the skills of hackers will be sharpened in the future.

## 5.0. Awareness Video

DDOS news

## References

1. Tolu, D. (2021). *Detection of Denial of Service Attack (DOS)*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/350873961_Detection_of_Denial_of_Servic e_Attack_DOS.
2. Johannes Ullrich (2020). *Exposed Windows Domain Controllers Used in CLDAP DDoS Attacks*. [online] Available at: https://isc.sans.edu/diary/Exposed+Windows+Domain+Controllers+Used+in+CLDAP+DDoS+Attacks/26526

 doi:10.20944/preprints202512.0440.v1




3. Tom Olzak. (2022). *How CLDAP Reflectors Enable DDoS Attacks & Ways to Reduce Your Exposure*. [online] Available at: https://www.spiceworks.com/it-security/cyber-risk-management/articles/defending-ag ainst-cldap-reflection-attacks/
4. Costa, J. and Robson (2024). Reflector Saturation in Amplified Reflection Denial of Service Attack Abusing CLDAP and Memcache Protocols. *Communications in computer and information science*, pp.248–263. doi:https://doi.org/10.1007/978-3-031-48855-9_19
5. Mohan, D. (2024). *What Are CLDAP Attacks? What Are The Risks And Impacts Of Such Attacks?* [online] Prophaze. Available at: https://prophaze.com/web-application-firewall/what-are-cldap-attacks/.
6. A Review of Amplification-based Distributed Denial of Service Attacks and Mitigation. (2021). *Computers & Security*, [online] p.102380. doi:https://doi.org/10.1016/j.cose.2021.102380.
7. Cybersecurity and Infrastructure Security Agency CISA. (2019). *DNS Amplification Attacks | CISA*. [online] Available at: https://www.cisa.gov/news-events/alerts/2013/03/29/dns-amplification-attacks.
8. Khormali, A., Park, J., Alasmary, H., Anwar, A., Saad, M. and Mohaisen, D. (2021). Domain name system security and privacy: A contemporary survey. *Computer Networks*, 185, p.107699. doi:https://doi.org/10.1016/j.comnet.2020.107699.
9. Learning Center. (n.d.). *What is Blackholing | Mitigating DDoS Attacks | Imperva*. [online] Available at: https://www.imperva.com/learn/ddos/blackholing/#:~:text=Blackholing%20involves%20redirecting%20traffic%20to.
10. Cloudflare. (n.d.) What is DDoS Blackhole Routing? [online] Available at: https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/.
11. Kumarasamy, S. (2011). Distributed Denial of Service (DDOS) Attacks Detection Mechanism. *International Journal of Computer Science, Engineering and Information Technology*, 1(5), pp.39–49. doi:https://doi.org/10.5121/ijcseit.2011.1504.
12. Zeb, K., Baig, O. and Asif, M.K. (2015). DDoS attacks and countermeasures in cyberspace. *2015 2nd World Symposium on Web Applications and Networking (WSWAN)*. doi:https://doi.org/10.1109/wswan.2015.7210322.
13. Mahajan, R., Bellovin, S.M., Floyd, S., Ioannidis, J., Paxson, V. and Shenker, S. (2002). Controlling high bandwidth aggregates in the network. *ACM SIGCOMM Computer Communication Review*, 32(3), pp.62–73. doi:https://doi.org/10.1145/571697.571724.
14. Mahajan, R., Bellovin, S.M., Floyd, S., Ioannidis, J., Paxson, V. and Shenker, S. (2002). Aggregate congestion control. *ACM SIGCOMM Computer Communication Review*, 32(1), p.69. doi:https://doi.org/10.1145/510726.510743.
15. Yaar, A., Perrig, A. and Song, D. (n.d.). *SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks* *. [online] Available at: https://users.ece.cmu.edu/~adrian/projects/siff.pdf [Accessed 19 Jun. 2024].
16. Azure, M. (2023) *Azure DDoS Protection—2021 Q3 and Q4 DDoS attack trends*. https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-at tack-trends/.
17. Heredia, R. (2021) 'What Are IoT Sensors? Types, Uses, and Examples,' *zipitwireless.com*, 30 August. https://www.zipitwireless.com/blog/what-are-iot-sensors-types-uses-and-examples.
18. Sharma, M. (2021) 'Microsoft Azure repels whopping 2.4 Tbps DDoS attack,' *TechRadar*, 12 October. https://www.techradar.com/news/microsoft-azure-repels-whopping-24-tbps-ddos-attac k.
19. IBM (2023). *What are Convolutional Neural Networks? | IBM*. [online] www.ibm.com. Available at: https://www.ibm.com/topics/convolutional-neural-networks.
20. Vyas.s, Nick.d, Oliver.s, Kobus.v, Hui.z (n.d.) Large-scale Automated DDoS detection SystemAvailable at: https://www.usenix.org/legacy/event/usenix06/tech/full_papers/sekar/sekar_html/ (Accessed: 28 June 2024).
21. Wiley Online Library (n.d.) Scientific Research Articles, journals, books, and reference works. Available at: https://onlinelibrary.wiley.com/ (Accessed: 28 June 2024).
22. Yunhe Cui *et al.* (2021) Towards ddos detection mechanisms in software-defined networking, Journal of Network and Computer Applications. Available at: https://www.sciencedirect.com/science/article/pii/S1084804521001703?casa_token= KZIDSOqZ4q8AAAAA%3A3ghw4yiWlPbBgrfmxGrVanhBDBLHTjFooQAklbqr4C_ lsERLNhKJ1EkvwPHEvIcEGAg9dumxRX7RJnA (Accessed: 28 June 2024).

 doi:10.20944/preprints202512.0440.v1




23. I. Cvitić, D. Perakovic, B. B. Gupta and K. -K. R. Choo, "Boosting-Based DDoS Detection in Internet of Things Systems," in IEEE Internet of Things Journal, vol. 9, no. 3, pp. 2109-2123, 1 Feb.1, 2022, doi: 10.1109/JIOT.2021.3090909. keywords: {Computer crime;Internet of Things;Smart homes;Servers;Feature extraction;Electronic mail;Telecommunication traffic;Artificial intelligence;cybersecurity;Distributed Denial of Service (DDoS);ensemble machine learning;IDS;Internet of Things (IoT);supervised learning},
24. Soodeh Hosseini a b et al. (2019) The hybrid technique for ddos detection with supervised learning algorithms, Computer Networks. Available at: https://www.sciencedirect.com/science/article/pii/S1389128618306881?casa_token=i_NAEHh4364UAAAAA%3ASVSZW2M8WHF2CEK_lTD0_5YWhvKGzg3RSBThiZ8XU5fyH3mnXtcRoYurWqCy1H9ykPNhDz0hORHppQ (Accessed: 28 June 2024).
25. Pande, S. et al. (1970) DDOS detection using machine learning technique, SpringerLink. Available at: https://link.springer.com/chapter/10.1007/978-981-15-8469-5_5 (Accessed: 28 June 2024).
26. S. S. Priya, M. Sivaram, D. Yuvaraj and A. Jayanthiladevi, "Machine Learning based DDOS Detection," 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2020, pp. 234-237, doi: 10.1109/ESCI48226.2020.9167642. keywords: {Computer crime;Servers;Classification algorithms;Machine learning;Computer hacking;Machine learning algorithms;Floods;Machine learning;DDoS detection},
27. GeeksforGeeks. (2019). Neural Networks | A beginners guide. [online] Available at: https://www.geeksforgeeks.org/neural-networks-a-beginners-guide/.
28. DeviceAuthority (2023). Symmetric Encryption vs Asymmetric Encryption: How it Works and Why it's Used. [online] Device Authority. Available at: https://deviceauthority.com/symmetric-encryption-vs-asymmetric-encryption/#:~:text=There%20are%20two%20 basic%20 types.
29. Learning Center. (n.d.). What is Blackholing | Mitigating DDoS Attacks | Imperva. [online] Available at: https://www.imperva.com/learn/ddos/blackholing/#:~:text=Blackholing%20involves%20redirecting%20traffic%20to.
30. Learning Center. (n.d.). What is Rate Limiting | Types & Algorithms | Imperva. [online] Available at: https://www.imperva.com/learn/application-security/rate-limiting/.
31. Lutkevich, B. (2021). What is a Digital Signature? [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/definition/digital-signature.
32. Ngo, Q.-D., Nguyen, H.-T., Nguyen, L.-C. and Nguyen, D.-H. (2020). A survey of IoT malware and detection methods based on static features. ICT Express, 6(4), pp.280–286. doi:https://doi.org/10.1016/j.icte.2020.04.005.
33. Microsoft (n.d.). Digital signatures and certificates - Microsoft Support. [online] Available at: https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96#
34. Kim, T.H. and Reeves, D. (2020). A survey of domain name system vulnerabilities and attacks. *Journal of Surveillance, Security and Safety*. doi:https://doi.org/10.20517/jsss.2020.14
35. Brooks, R.R., Ozcelik, I., Yu, L., Oakley, J. and Tusing, N. (2021). Distributed Denial of Service (DDoS): A History. *IEEE Annals of the History of Computing*, pp.1–1. doi:https://doi.org/10.1109/mahc.2021.3072582
36. Alcoz, A.G., Strohmeier, M., Lenders, V. and Vanbever, L. (2022). Aggregate-based congestion control for pulse-wave DDoS defense. *Proceedings of the ACM SIGCOMM 2022 Conference*. [online] doi:https://doi.org/10.1145/3544216.3544263.
37. docs.aws.amazon.com. (n.d.). *UDP Reflection Attacks - AWS Best Practices for DDoS Resiliency*. [online] Available at: https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/udp-reflection-attacks.html.
38. GlobalDots, P.K., Solutions Engineer @ (2023). *How DDoS Works: Beginners Guide*. [online] GlobalDots. Available at: https://www.globaldots.com/resources/blog/how-ddos-works/ [Accessed 28 Jun. 2024].
39. Ibeakanma, C. (2022). *What Are TCP and UDP Ports?* [online] MUO. Available at: https://www.makeuseof.com/what-are-tcp-and-udp-ports/.
40. IBM (2022). *What is Ransomware?* [online] www.ibm.com. Available at: https://www.ibm.com/topics/ransomware.

41. IBM (2023). *What are Convolutional Neural Networks? | IBM*. [online] www.ibm.com. Available at: https://www.ibm.com/topics/convolutional-neural-networks.
42. Mariani, V. (2022). *What is an Internet Filtering Software and why it is used*. [online] FlashStart. Available at: https://flashstart.com/internet-filtering-software-what-it-is-and-why-it-is-used/.
43. Namane, S., Ahmim, M., Kondoro, A. and Dhaou, I.B. (2023). Blockchain-Based Authentication Scheme for Collaborative Traffic Light Systems Using Fog Computing. *Electronics*, 12(2), p.431. doi:https://doi.org/10.3390/electronics12020431.
44. Newman, L. (2018). *A 1.3-Tbs DDoS Hit GitHub, the Largest Yet Recorded*. [online] WIRED. Available at: https://www.wired.com/story/github-ddos-memcached/.
45. www.radware.com. (n.d.). *What is rate limiting and how does it work? | Radware*. [online] Available at: https://www.radware.com/cyberpedia/bot-management/rate-limiting/.
46. Yang, H. and Li, Y. (2022). A Blockchain-Based Anonymous Authentication Scheme for Internet of Vehicles. *Procedia Computer Science*, 201, pp.413–420. doi:https://doi.org/10.1016/j.procs.2022.03.109.
47. Lopez-Martin, M. *et al.* (2017) 'Network traffic classifier with convolutional and recurrent neural networks for internet of things', *IEEE Access*, 5, pp. 18042–18050. doi:10.1109/access.2017.2747560.
48. Radford, B.J. *et al.* (2018) *Network traffic anomaly detection using recurrent neural networks*, *arXiv.org*. Available at: https://doi.org/10.48550/arXiv.1803.10769
49. Meng, W., Li, W. and Zhou, J. (2021) 'Enhancing the security of blockchain-based software defined networking through Trust-based traffic fusion and filtration', *Information Fusion*, 70, pp. 60–71. doi:10.1016/j.inffus.2020.12.006.
50. Zheng, Z. *et al.* (2018) 'Blockchain challenges and opportunities: A survey', *International Journal of Web and Grid Services*, 14(4), p. 352. doi:10.1504/ijwgs.2018.095647.
51. Khalil, M. I., Humayun, M., Jhanjhi, N. Z., Talib, M. N., & Tabbakh, T. A. (2021). Multi-class segmentation of organ at risk from abdominal ct images: A deep learning approach. In Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2021 (pp. 425-434). Singapore: Springer Nature Singapore.
52. Humayun, M., Jhanjhi, N. Z., Niazi, M., Amsaad, F., & Masood, I. (2022). Securing drug distribution systems from tampering using blockchain. Electronics, 11(8), 1195.
53. Sama, N. U., Zen, K., Jhanjhi, N. Z., & Humayun, M. (2024). Computational Intelligence Ethical Issues in Health Care. In *Computational Intelligence in Healthcare Informatics* (pp. 349-362). Singapore: Springer Nature Singapore.
54. Yan, O. J., Ashraf, H., Ihsan, U., Jhanjhi, N., & Ray, S. K. (2024, January). Facial expression recognition (FER) system using deep learning. In *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)* (pp. 1-11). IEEE.
55. Tayyab, M., Hameed, K., Jhanjhi, N. Z., Zaheer, A., & Qamar, F. (2024). Digital safeguards: Navigating cyber threats in the logistics industry framework. In *Navigating cyber threats and cybersecurity in the logistics industry* (pp. 258-299). IGI Global Scientific Publishing.
56. Khandelwal, M., Rout, R. K., Umer, S., Sahoo, K. S., Jhanjhi, N. Z., Shorfuzzaman, M., & Masud, M. (2023). A Pattern Classification Model for Vowel Data Using Fuzzy Nearest Neighbor. *Intelligent Automation & Soft Computing*, *35*(3).
57. Pandian, M. T., Chouhan, K., Kumar, B. M., Dash, J. K., Jhanjhi, N. Z., Ibrahim, A. O., & Abulfaraj, A. W. (2022). RETRACTED: Improving Efficiency of Large RFID Networks Using a Clustered Method: A Comparative Analysis. *Electronics*, *11*(18), 2968.
58. Humayun, M., Sujatha, R., Almuayqil, S. N., & Jhanjhi, N. Z. (2022, June). A transfer learning approach with a convolutional neural network for the classification of lung carcinoma. In *Healthcare* (Vol. 10, No. 6, p. 1058). MDPI.
59. Srinivasan, K., Garg, L., Alaboudi, A. A., Jhanjhi, N. Z., Prabadevi, B., & Deepa, N. (2021). Expert System for Stable Power Generation Prediction in Microbial Fuel Cell. *Intelligent Automation & Soft Computing*, *30*(1).
60. Saeed, S., Jhanjhi, N. Z., Abdullah, A., & Naqvi, M. (2018). Current Trends and Issues Legacy Application of the Serverless Architecture. *International Journal of Computing Network Technology*, *6*(3).

 doi:10.20944/preprints202512.0440.v1




61. Javed, D., Jhanjhi, N. Z., Ashfaq, F., Khan, N. A., Das, S. R., & Singh, S. (2024, July). Student Performance Analysis to Identify the Students at Risk of Failure. In *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 1-6). IEEE.
62. Jhanjhi, N. Z., Gaur, L., & Khan, N. A. (2024). Global Navigation Satellite Systems for Logistics: Cybersecurity Issues and Challenges. *Cybersecurity in the Transportation Industry*, 49-67.
63. Khan, M. R., Khan, N. R., & Jhanjhi, N. Z. (Eds.). (2024). *Convergence of Industry 4.0 and supply chain sustainability*. IGI Global.
64. Ashraf, H., Jhanjhi, N. Z., Brohi, S. N., & Muzafar, S. (2024). A Comprehensive Exploration of DDoS Attacks and Cybersecurity Imperatives in the Digital Age. In *Navigating Cyber Threats and Cybersecurity in the Logistics Industry* (pp. 236-257). IGI Global Scientific Publishing.
65. Qasim, M., Mahmood, D., Bibi, A., Masud, M., Ahmed, G., Khan, S., ... & Hussain, S. J. (2022). PCA-based advanced local octa-directional pattern (ALODP-PCA): a texture feature descriptor for image retrieval. *Electronics*, *11*(2), 202.
66. Manzoor, M. K., Latif, R. M. A., Haq, I., & Jhanjhi, N. Z. (2022). An energy-efficient routing protocol via angle-based flooding zone in underwater wireless sensor networks. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(2s), 116-123.
67. Gill, S. H., Sheikh, N. A., Rajpar, S., Jhanjhi, N. Z., Ahmad, M., Razzaq, M. A., ... & Jaafar, F. (2021). Extended Forgery Detection Framework for COVID-19 Medical Data Using Convolutional Neural Network. *Computers, Materials & Continua*, *68*(3).