Detecting Ddos Attack Using Deep Learning Techniques

Puvaneswaran M[1], Parthipan P[2], S Nivetha[3]

[1,2]Student, B.E Computer Science and Engineering with Artificial Intelligence, Sathyabama Institute of Science and Technology, Semmancheri, Chennai, TamilNadu, India-600119
[3]Assistant Professor, Department of Computer Science and Engineering,Sathyabama Institute of Science and Technology, Semmancheri, Chennai,TamilNadu, India-600119

Abstract

In the modern digital world, the robustness of cybersecurity frameworks is crucial for maintaining operational integrity and safeguarding organizational assets. Distributed Denial of Service (DDoS) attacks are a frequent and very destructive kind of cyber intrusion that must be recognized and avoided, this study presents a Deep Learning. Based Intrusion Detection System (IDS). Distributed Denial of Service (DDOS)flooding is one of the security flaws that seriously damages IoT systems. DDOS assaults cannot be prevented by conventional data filtering methods. To safeguard the security of IoT settings, a novel hybrid deep CNN model-based framework for identifying DDoS flooding assaults is put forth in this study. It is utilized to satisfy the security needs of IoT settings and to overcome the drawbacks of existing DDoS attack detection approaches. One dimensional (1D) CNN and two dimensional (2D) CNN are used with two and three convolutional layers, respectively, to build a Hybrid Deep CNN model.

Keywords – Distributed Denial of Service attack, Convolutional Neural Networking

Introduction

DDoS threats have escalated, with an estimated 75.4 devices by 2025.Insecure pairing processes, unsecured storage, unencrypted communications, vulnerable online, mobile, and cloud interfaces, and even hardcoded backdoors are present in the majority of these devices, if not all of them, making them prime targets for hackers to target and use for their own ends. In order to overload targets, denial of service (DoS) and DDoS assaults both employ fake or sometimes extremely high traffic volumes. DoS attacks, which one or more attackers may execute, concentrate on specific servers or endpoints rather than the entire network. DDoS attacks flood systems with data using a number of dispersed devices. Targets include the hardware and protocols used to connect the network to the internet. The following are types of DoS attacks: Single-source SYN floods: DDoS attack that involves a single attacker attempting to overload a target system with a huge quantity of SYN packets so that genuine users are unable to access it.

Ping of Death (PoD): A PoD attack is a form of DoS attack in which the attacker sends a packet that exceeds the target machine's maximum permissible size in an effort to stop it from operating or cause it to halt or collapse. Nowadays, there are fewer instances of the original ping of death attack. There is a more common assault akin to this one called an ICMP flood attack.

Slowloris assault: Because it targets a particular web server, the slowloris attack is technically a typical DoS attack, although being commonly referred to as a DDoS attack, and it commonly does not employ intermediary networking devices. While considering the types of DDoS attacks, there are three general types which are Application layer attacks, Protocol attacks and Volumetric attacks. It is still challenging to provide widespread protection against volumetric DDoS attacks with zero latency. Cybercriminals have developed advanced tools to carry out enormous DDoS assaults as a result of technological breakthroughs. These sophisticated DDoS

assaults compromise data privacy and the operation of network infrastructure by interfering with information transit between the network and transport levels.

Massively volumetric attack methods like NTP amplification, DNS amplification, UDP flood, and TCP flood leverage the whole bandwidth of networks and resources. Providers of DDoS prevention and mitigation solutions need to have a proactive defensive mechanism for network- and application-level services since DDoS attack technologies are always evolving. To safeguard the integrity and confidentiality of data that is vital to their operations, businesses are encrypting their network communication methods. Businesses are using Secure Sockets Layer (SSL)encrypted technology to counteract DDoS assaults at the network and transport layers as internet usage increases. Businesses find it difficult to discern between harmful and legitimate communication as fraudsters are using SSL to launch DDoS attacks against traffic that is SSL encrypted. DDOS assaults are too complicated for malware detection technologies to detect. To avoid such covert DDoS assaults, DDOS prevention and mitigation solution vendors must thereby overcome major challenges.

Scope

How well various DDoS detection methods work, as well as how well they can recognise and stop DDoS attacks. The performance of several DDoS detection methods in various contexts is explained in depth. Online services' performance and availability when subjected to DDoS assaults, as well as how well various detection methods work to lessen these effects. Methods for overcoming the difficulties involved in setting up and maintaining DDoS detection systems. An analysis of effective DDoS detection system implementations by companies, together with insights gained from their experiences. The Zero Trust architecture incorporates intrusion detection systems, firewalls, and DDoS and insider threat detection.

DDoS detection's function in adhering to rules and industry norms. IoT devices' low resources and incapacity to manage high traffic volumes make them especially susceptible to DDoS assaults. Organisations must have robust security measures in place and have a plan in place for responding to and mitigating DDoS assaults in order to defend against DDoS attacks on IoT devices. Network traffic analysis, intrusion detection systems (IDS), web application firewalls (WAF), load balancers, and cloud-based DDoS security services are some methods for identifying DDoS assaults. Businesses may help shield themselves and their clients from the negative consequences of DDoS assaults by using these strategies and taking the necessary precautions

Literature Survey

2.1Introduction

In today's digital environment, insider threats and distributed denial of service (DDoS) assaults are two serious hazards that organizations must deal with. DDoS assaults are a kind of cyberattack in which the attacker floods a network or website with traffic, preventing authorized users from accessing it. Insider dangers, on the other hand, refer to the potential risk of harm to an organization that may come from within, such as from its employees, contractors, or other trusted insiders. To detect and mitigate these threats, organizations can use a combination of technical and non-technical approaches. For DDoS attacks, this may include techniques such as network traffic analysis, Intrusion Detection Systems (IDS), and Web Application Firewalls (WAF). Organizations may utilize access controls, employee behavior tracking, and routine security assessments to identify insider risks. It is important for organizations to have a robust and multi-faceted approach to detecting and mitigating DDoS attacks and insider threats, as these threats can have significant consequences for an organization, including disruption of business operations, reputational harm as well as monetary loss. This thesis's thorough analysis of the state

The most advanced methods for detecting DDoS attacks and insider threats were examined. 20 2.2 DDoS DETECTION DDoS attacks are becoming more common as the demand for Internet connectivity has increased rapidly in recent years due to recent advances in wireless technology and cutting-edge computing paradigms. This chapter aims to discuss the previous research findings on the topic of DDoS attacks. It provides a comprehensive analysis of the existing DDoS attacks and vulnerabilities which have already been identified by researchers, as well as a description of the novel approaches and architectures. In addition, the understanding of DDoS attacks as well as the detection in pertaining to the research are discussed in this section. Dong and Sarem (2019) introduced a DDoS detection method as a new dimension to evaluate defense against DDoS attacks. Recent DDoS attack detection methods resulted in low accuracy and are vulnerable to other factors. The proposed method based on the Degree of Attack is used to compute the degree of attack for identifying DDoS attacks as well as the classifications are performed using ML techniques. Improved K- Nearest Neighbors (KNN) algorithm is used to classify the normal and malicious traffic. Initially, DDoS patterns are identified with major features such as flow duration, flow length, flow size and flow ratio to assess DDoS attack detection performance.

The outcomes of the experiment showed that the suggested approach could effectively identify DDoS assaults and get greater detection rates (Dong & Sarem 2019). A DoS and DDoS Attacks Detection Algorithm for computer networks is developed using the ARIMA Time Series Model and Chaotic System (Tabatabaie Nezhad et al., 2016). Initially, two detection metrics—the quantity of packets and source IP addresses—are extracted from network traffic every minute. The time series is constructed using a Box-Cox transformation based on the number of packets in order to normalize it.

A lightweight model for the Internet of Things environment is proposed to detect DDoS malware (Su et al., 2018). By using image recognition algorithms with grayscale pictures taken from malware binaries, a well- defined convolutional neural network is constructed to identify the malware families. Machine learning classifiers use the resulting grayscale pictures as input. The distant cloud server receives any harmful files found for further analysis. Because it includes details on every malware sample, the signature matching system's database is enormous. As a result, IoT devices' resources are limited and fixed, which is inefficient for the IoT ecosystem. To offer 22 lightweight malware detection and identify harmful activity with a 94.0% accuracy rate, a small, two-layered shallow CNN is needed. It is suggested to use a classifier system called CS DDoS to identify and stop DDoS TCP flood attacks on public clouds (Sahi et al., 2017).

By classifying incoming packets and making decisions based on the classification findings, the proposed CS DDoS system provides a way to secure stored records. The CS DDOS detects and assesses during the detection phase whether a packet is normal or comes from an attacker. Malicious packets will not be allowed access to the cloud service during the preventive phase, and the source IP will be blacklisted. Utilizing the different classifiers of the Least Squares Support Vector Machine LS-SVM, naive Bayes, K-nearest, and multilayer perceptron, the performance of the CS DDoS system is compared. The findings show that CS DDoS achieves the best effectiveness when the LS-SVM classifier is applied. It can identify DDoS TCP flood assaults with around 97% accuracy and a Kappa coefficient of 0.89 when attacked by a single source; when attacked by several sources, it can identify them with 94% accuracy and a Kappa coefficient of 0.9.

NB-MAIDS was presented by Mehmood et al. (2018) with the goal of improving intrusion detection accuracy by using IoT network behaviours for feature selection. Detection and prevention of DDoS attack traffic coming from devices connected to the home network are the primary objectives of NB-MAIDS. For pattern matching, the light-weighted Naive Bayes classification method is essential for intrusion detection systems. Performance is enhanced when the NB approach is applied with a large number of agents. DDoS attacks from hostile sources target the secured layers of IoT networks. The results of the trial showed that 91-99% detection accuracy was achieved.

A cross-domain attack detection method has been developed to improve the efficacy of denial-of-service attack detection in Software Defined Networks (SDNs) (Zhu et al., 2018). Each SDN's domain must provide a significant quantity of real traffic data in order to be detected, albeit this data may leak sensitive information.

Predis, a cross-domain attack detection technique for SDNs that protects privacy, is suggested. Predis uses k- Nearest Neighbors (KNN), a computationally simple and effective method, as its detection algorithm to preserve privacy by integrating perturbation encryption with data encryption. To improve efficiency, KNN is enhanced, by rigorous simulations and theoretical study. Predis has demonstrated its ability to identify attacks effectively and accurately while protecting each domain's sensitive data.

DDoS Flooding Detection Framework

This section describes the elements of the proposed DDoS flooding detection framework for IoT environment. When a DDoS assault overwhelms a target server, service, or network with a massive amount of internet traffic, it disrupts the normal flow of traffic on that machine or system. The effectiveness of DDoS assaults is increased by leveraging different compromised computer systems as the main sources of attack traffic. Furthermore, the network's compromised devices and systems are under the remote control of the attackers (Simplício et al., 2017). The terms "bots" and "zombies" describe individual hacked devices, whereas "botnet" describes a group of bots. It is common practice to employ traffic analytics tools to identify some of the unique signs of a DDoS assault.

Massive user traffic flooding, unusual traffic patterns, and unexpectedly high traffic volumes coming from a single IP address or IP range are all signs of a DDoS attack (Simplício et al., 2017; Angrishi 2017; www.av- test.org/fileadmin/pdf/security_report/AVTEST_Security_Report_2019-2020; Su et al., 2018). There are three types of DDoS assaults: application-layer attacks (like an HTTP flood), protocol-level attacks (like a SYN flood), and volumetric attacks (like DNS amplification). Application layer attacks target the section of the web server architecture where, web pages are generated and transmitted as HTTP requests and responses. Protocol attacks cause service disruptions by utilising excessive server resources as well as network equipment resources like firewalls and load balancers.

By completely consuming the available bandwidth between the target and the main network, volumetric attacks attempt to block up the Internet (Hemalatha et al., 2021). To launch DDoS flood attack, attackers first remotely control the IoT devices such as cameras, sensors, smart-watches, printers and so on. After that malicious requests are sent towards target servers by utilizing their resources like connectivity and battery power forcefully. Then targeted servers are continuously overwhelmed by DDoS flood attack. In the meantime, legitimate users will not get their desired services due to the impact of the attack. Figure 3.9 depicts the attack scenario in IoT environment.

The following list includes the research's main contributions.

1. System for detecting DDoS flooding attacks based on the Deep CNN model is suggested.
2. In the proposed Deep CNN model, 1D CNN is utilized for effective feature extraction and 2D CNN is utilized classifying and identifying DDoS flooding.

Proposed Diagram

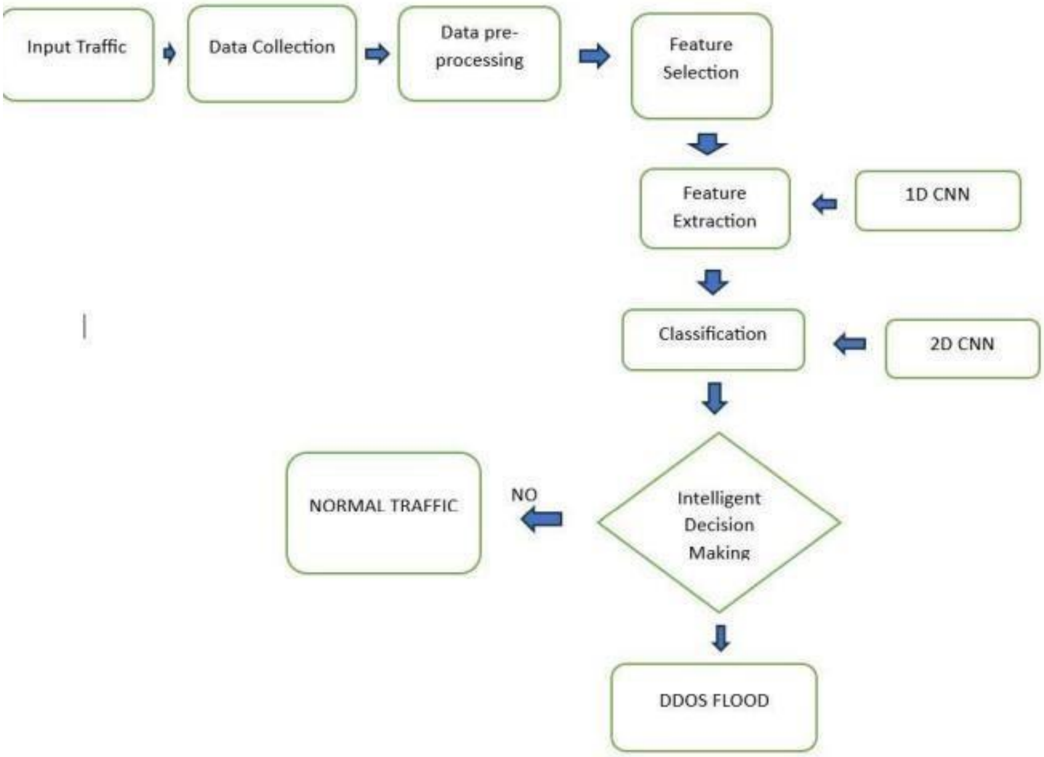

FIGURE 4.2.1.1 DDOS PROPOSED WORK

Data collection

The process of conducting research requires data. Therefore, getting such information from a trustworthy source is essential. To understand what a dataset is, one must look at its constituent parts.Videos,music, and text are just a few of the formats it might be in.
(www.marketsandmarkets.com/pdfdownloadNew.asp?id=67064836&utm),BIG2015
(www.cloudflare.com/en-in/learning/ddos/glossary/mirai-botnet/), Malevis (Roopak et al., 2020), and Malicia (Hussain 2020) are four large datasets that are frequently used in the field of malware detection and classification to locate and classify malware.

Data Pre-Processing

To finish the dataset and remove noise, pre-processing is a vital and essential stage. It is used to carry out precise data analysis and, in the end, get the best result. Artefacts that show up in a traffic but do not originate from the original source's content are referred to as noise in the data (Tu et al., 2020). A statistical change in a measurement brought on by a random process is often referred to as noise. Throughout the whole data set, noise manifests as a grainy structure and an artefact over the flow. Noise is an unwanted or upsetting event that generally lowers the subjective quality of any data. It is challenging to eliminate noise as it is essentially connected to the high-frequency content, also known as the details. Therefore, the objective is to develop a system that minimises background noise while maintaining the greatest amount of information.

Classification using 1D CNN

When categorizing input traffic in an IoT environment, these extracted features are employed to ensure accuracy. CNN is made up of two main parts: feature extraction and feature categorisation. The CNN feature extraction component is in charge of automatically determining the best characteristics from the input traffic in an Internet of Things context. The primary goal of CNN is accomplished by these two CNN components.

Feature extraction in CNN is comprised of a convolution layer and a sampling layer. In order to improve the qualities of the incoming traffic, the convolution layer's fuzzy filter reduces data noise. The current layer convolution kernel layer and the upper layer feature vector are utilised to 99 carry out the convolution. Calculations for the convolution process are actually completed by CNN's activation function.

Classification using 2D CNN

Since one-dimensional signals lack flexibility, the one-dimensional convolutional neural network is commonly employed. This issue is resolved by converting input traffic into a two-dimensional format. Due to their lower error rate, the 2D kernels in the 2D CNN models may be used to represent the time series data. There are several trustworthy techniques that may be used to represent 2D data in a unique way. The continuous wave transform method is adjusted to use a 2D CNN to capture the input data's microstructural information. A Continuous Wavelet transform (CWT) can efficiently describe non-stationary information with changeable instantaneous frequency in its frequency domain. The CWT is capable of characterising the frequency and localised amplitude of time-varying signals.

Result and Discussion

In entire experimentation is performed in the secured cloud with multi-tenant architecture running B2S machine in Azure cloud with Windows Server 2022 data centre edition. The cloud is architect in such a way that it forms the multitenant fashion. The data collected is a real time data in NSL KDD format. This is to ensure the benchmark of the proposed system. DDoS tools such as Tor Hammer, HULK are used to perform the DDoS attack. Figure 4.1 shows the total attack statistics.

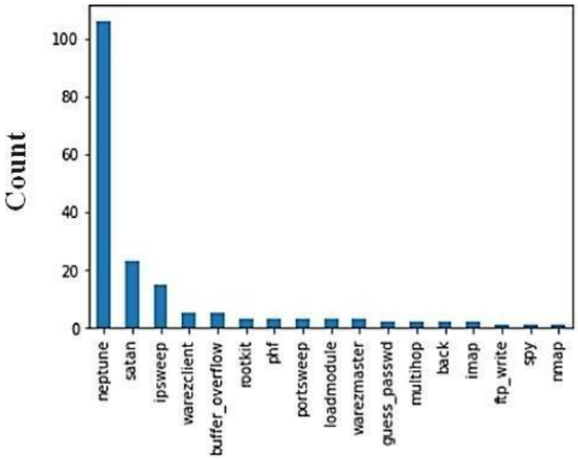

Figure 4.1 Attack Statistics

Confusion Matrix

A Confusion Matrix is a performance evaluation tool used to gauge a model's accuracy in machine learning and classification tasks. With important metrics like True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN), it offers a tabular depiction of expected vs actual results. erroneously predicted positives are denoted by FP, erroneously forecasted negatives by FN, correctly predicted positives by TP, and properly predicted negatives by TN**.**

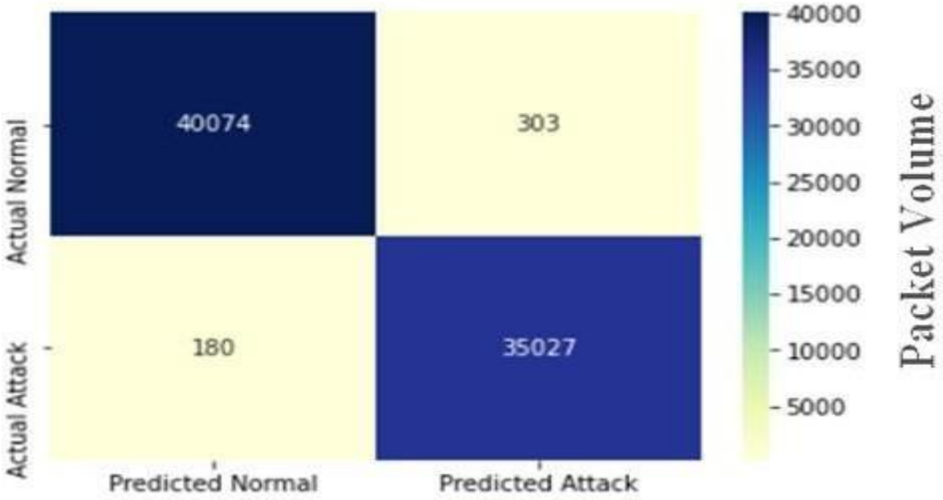

Figure 4.2 Confusion metrics

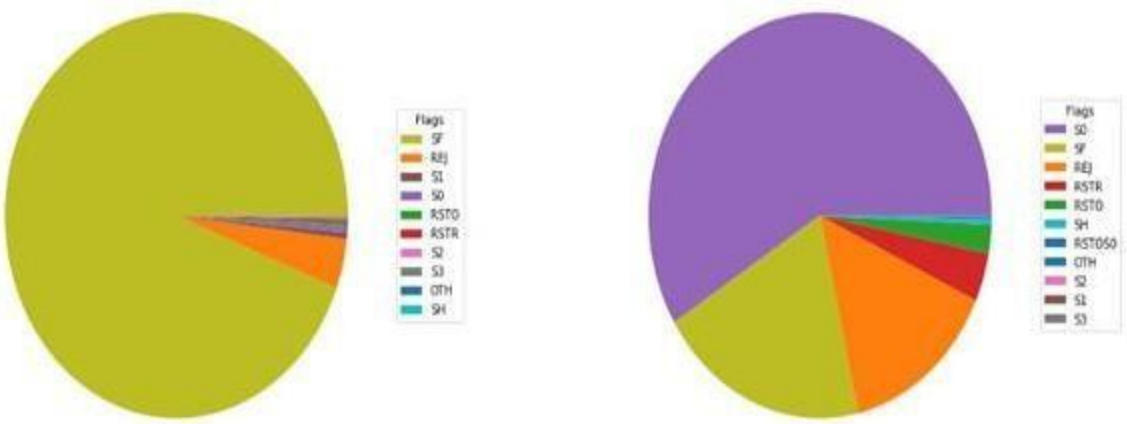

Figure 4.3 Statistics of Normal and Attack Conditions

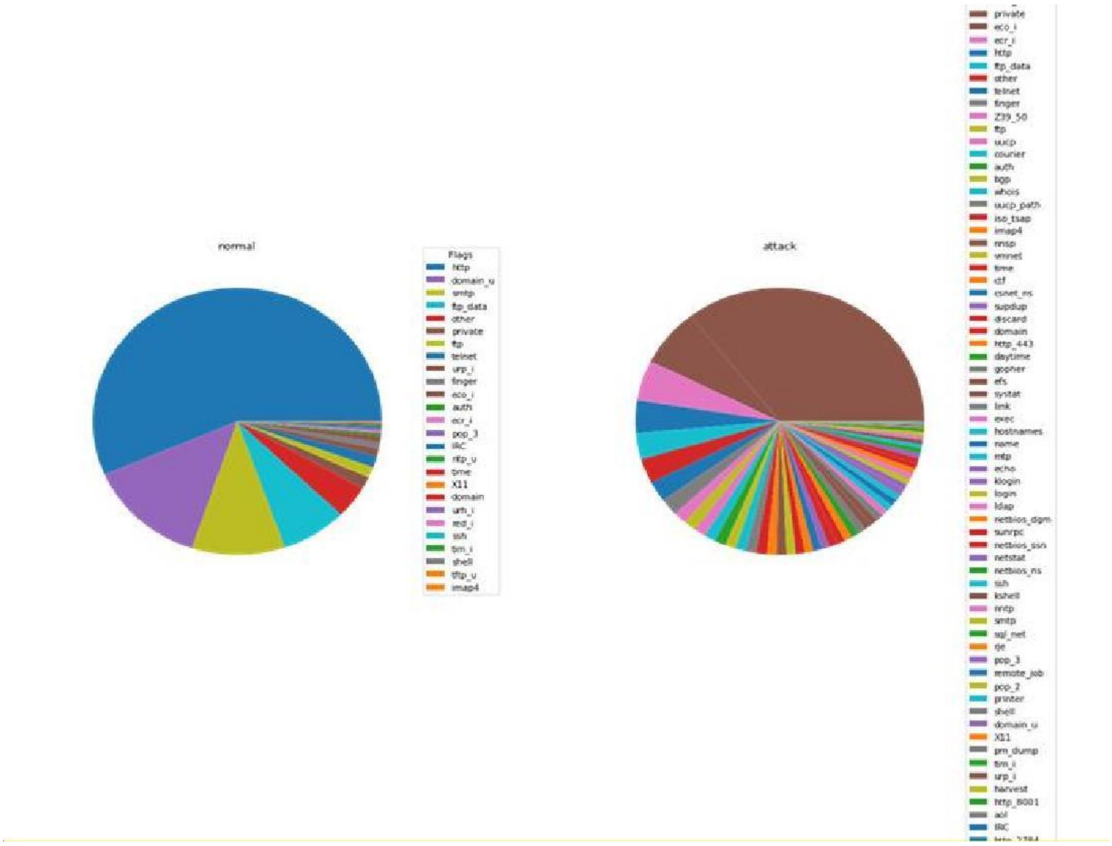

Figure 4.4 Overall, Packet Statistics

Conclusion

In order to meet the security needs of the Internet of Things environment, a deep hybrid CNN model-based framework for detecting DDoS flooding assaults is developed. Considering the limitations of existing approaches, this novel detection framework will overcome them. One of the security risks that has a major influence on IoT systems is distributed denial of service (DDoS) floods. A hybrid deep convolutional neural network model is constructed using a one-dimensional CNN with two convolutional layers and a two- dimensional CNN with three convolutional layers. The CWT is used to transform data binary files to 2D so that unwanted and superfluous information may be eliminated from the traffic data without compromising crucial information.

Reference

1. Al-Shareeda, Mahmood A., Selvakumar Manickam, and Murtaja Ali Saare. "DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison." Bulletin of Electrical Engineering and Informatics 12.2 (2023): 930-939
2. Mittal, Meenakshi, Krishan Kumar, and Sunny Behal. "Deep learning approaches for detecting DDoS attacks: A systematic review." Soft computing 27.18 (2023): 13039-13075.
3. Bindra, Naveen, and Manu Sood. "Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset." Automatic Control and Computer Sciences 53.5 (2019): 419-428.
4. Wani, Abdul Raoof, et al. "Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques." 2019 Amity International conference on artificial intelligence (AICAI). IEEE, 2019.
5. Arshi, M., M. D. Nasreen, and Karanam Madhavi. "A survey of DDoS attacks using machine learning techniques." E3S Web of Conferences. Vol. 184. EDP Sciences, 2020.
6. Pande, Sagar, et al. "DDOS detection using machine learning technique." Recent Studies on Computational Intelligence: Doctoral Symposium on Computational Intelligence (DoSCI 2020). Springer Singapore, 2021.
7. Ali, Tariq Emad, Yung-Wey Chong, and Selvakumar Manickam. "Machine learning techniques to detect a DDoS attack in SDN: A systematic review." Applied Sciences 13.5 (2023): 3183.
8. Khempetch, Thapanarath, and PongpisitWuttidittachotti. "DDoS attack detection using deep learning." IAES International Journal of Artificial Intelligence 10.2 (2021): 382.
9. Tuan, Tong Anh, et al. "Performance evaluation of Botnet DDoS attack detection using machine learning." Evolutionary Intelligence 13.2 (2020): 283-294.
10. BanitalebiDehkordi, Afsaneh, MohammadRezaSoltanaghaei, and Farsad Zamani Boroujeni. "The DDoS attacks detection through machine learning and statistical methods in SDN." The Journal of Supercomputing 77.3 (2021): 2383-2415.
11. Rahman, Obaid, Mohammad Ali Gauhar Quraishi, and Chung-Horng Lung. "DDoS attacks detection and mitigation in SDN using machine learning." 2019 IEEE world congress on services (SERVICES). Vol. 2642. IEEE, 2019.
12. Sadhwani, Sapna, et al. "A lightweight model for DDoS attack detection using machine learning techniques." Applied Sciences 13.17 (2023): 9937.
13. Yungaicela-Naula, Noe Marcelo, Cesar Vargas-Rosales, and Jesus Arturo Perez-Diaz. "SDN- based architecture for transport and application layer DDoS attack detection by using machine and deep learning." IEEE Access 9 (2021): 108495-108512.\
14. Aktar, Sharmin, and Abdullah Yasin Nur. "Towards DDoS attack detection using deep learning approach." Computers & Security 129 (2023): 103251.
15. Almaraz-Rivera, Josue Genaro, Jesus Arturo Perez-Diaz, and Jose Antonio Cantoral-Ceballos. "Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models." Sensors 22.9 (2022): 3367.
16. Polat, Huseyin, Onur Polat, and Aydin Cetin. "Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models." Sustainability 12.3 (2020): 1035.

17. Cil, Abdullah Emir, Kazim Yildiz, and Ali Buldu. "Detection of DDoS attacks with feed forward based deep neural network model." Expert Systems with Applications 169 (2021): 114520.
18. Boonchai, Jirasin, KotcharatKitchat, and SarayutNonsiri. "The classification of DDoS attacks using deep learning techniques." 2022 7th International Conference on Business and Industrial Research (ICBIR). IEEE, 2022.
19. Başkaya, Dilek, and Refi Samet. "Ddos attacks detection by using machine learning methods on online systems." 2020 5th International Conference on Computer Science and Engineering (UBMK). IEEE, 2020.
20. Ahmed, Sheeraz, et al. "Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron." Future Internet 15.2 (2023): 76.