Int. J. Advance Soft Compu. Appl, Vol. 18, No. 2, July 2026
Print ISSN: 2710-1274, Online ISSN: 2074-8523

An Intelligent Approach to HTTP Flood DDoS Detection Using Bayes-Entropy

Kamal Alieyan[1], Saad Ismail[1], Ayman Ghaben[1], Adnan Shaout[2], Mohamed S. Sawah [3,4]*,Ahmed E Fakhry[1,5]

[1]College of Information Technology, Amman Arab University, Amman 11953, Jordan, k.alieyan@aau.edu.jo, s.ismail@aau.edu.jo, a.ghaben@aau.edu.jo
[2]The Electrical and Computer Engineering Department, The University of Michigan Dearborn,Dearborn, MI 48128, USA, shaout@umich.edu
[3]Department of Data Science and Artificial Intelligence, Faculty of Information Technology, Ajloun National University P.O.43, Ajloun-26810, JORDAN, m.elsawah@anu.edu.jo
[4]Department of Information Systems, Al-Alson Higher Institute, Cairo, Egypt.
[5]Faculty of Information Systems and Computer Science, October Six University, Giza, Egypt, a.elsharkawy@aau.edu.jo

* Corresponding author: Mohamed S. Sawah

Abstract

One of the most serious cyberattacks on network systems or internet services is the distributed denial of service (DDoS) attack. To stop destructive HTTP flooding DDoS packets from reaching the website, this work presented a powerful mathematical approach based on Bayes-entropy. This technique will use the Bayes theorem to calculate the chance of HTTP flooding DDoS attacks inside the group and the entropy equation to calculate the unpredictability within the group. The main novelty of this work lies in introducing a unified Bayes-entropy detection mechanism that jointly measures attack probability and traffic randomness at the event-group level within aggregated HTTP packets. Unlike existing methods that typically rely on either probability-based analysis or entropy-based analysis alone, the proposed approach combines both measures in a single mathematical framework to reduce misclassification between normal and HTTP flooding DDoS traffic and improve detection accuracy. Experimental results on the ISCX dataset show that the proposed method achieved an accuracy of 97.14%, a true-positive rate of 92.85%, a true-negative rate of 100%, a false-positive rate of 0%, and a false-negative rate of 7.14%, confirming the reliability and effectiveness of the proposed Bayes-entropy detection mechanism.

Keywords: *DDoS attacks, HTTP flooding, online services, quantitative metrics, networking security.*

1 Introduction

The dependence on the internet for all aspects of human life have increased exponentially over the past few years. Growth is being fueled by demand across all verticals (public and private), and the pervasive utilization of emerging technologies like smart mobile devices, financial technology (fntech), advanced communication technologies, and the Internet of Things along with solutions [1]. However, the explosive growth of Internet-connected devices and applications has introduced a host of new worries, including greater risk of cyber threats of all kinds, please see [2]. The most common types of cyber-attacks are denial of service (DoS) and distributed denial of service (DDoS) attacks. These exploits are intended to use the access of a normal user to network services or resources to the attacker's advantage. This leads to the need for significant investment of time and money in many companies to secure and protect their network services from such kind of attacks.

Detection and mitigation of these attacks is challenging since they are changing pattern attacks and also the DoS/DDoS patterns of attack traffic are very close to the normal network traffic patterns. Consequently, an understanding of the DoS/DDoS attacks nature is required before an appropriate effective countermeasure can be designed and applied. People, companies and governments are all at risk to DoS and DDoS attacks, as [3]. Continuous attacks on company servers and ISPs illustrate that DoS attacks are a persistent threat on the internet. Because of the network outage, many customers were unable to access online services and crucial network resources such as cloud services, web servers, e-mail servers, and domain name resolvers, see [4]. DDoS attacks, on the other hand, are the most dangerous since they deprive real users of internet services or resources, as [5]. The first well-documented DDoS attack appears to have occurred in August 1999. On February 7, the following year, the Yahoo! Internet portal was unavailable for three hours due to what was then considered the first large-scale DDoS attack. Amazon, Buy.com, CNN, and eBay were all attacked by DDoS attacks the next day, rendering their web servers [6].

This mechanism's main contribution is combining the Bayes theorem and the entropy equation to apply them together on each event of the aggregated packets in the traffic, which will be enhancing the previous HTTP flooding DDOS attack mechanisms by utilizing logical, statistical, probability, and calculus functions, thus increasing the classification accuracy of this mechanism, which implies it improves the overall detection accuracy of the proposed mechanism. Please see [7-8].

Despite the large number of existing studies on HTTP flooding DDoS detection, the current literature still shows an important research gap. Many previous approaches focus on only one aspect of the traffic behavior, such as probability-based analysis or entropy-based randomness analysis, while others rely on machine learning or statistical models that may not jointly capture both the likelihood of attack occurrence and the uncertainty of packet behavior. As a result, existing studies are not always sufficient to clearly distinguish normal HTTP traffic from flooding DDoS traffic, which may lead to misclassification and reduced detection accuracy. Therefore, there is a need for a unified mathematical mechanism that combines

Bayes' theorem and entropy within the same detection framework to provide a more reliable and accurate identification of HTTP flooding DDoS attacks.

The objective of this study is to develop an accurate mathematical mechanism for detecting HTTP flooding DDoS attacks in network traffic. Specifically, the study aims to combine Bayes' theorem and the entropy equation within a unified Bayes-entropy framework applied to the events of aggregated packets, in order to jointly measure attack probability and traffic randomness, reduce misclassification between normal and malicious traffic, and improve the overall detection accuracy of HTTP flooding DDoS attacks.

The rest of this paper is organized as follows: Section 2 explains the research's context. Section 3: Corresponding works. The Proposed Mechanism is covered in Section 4. Section 5: An illustrative example. Section 6 presents the experimental results before concluding this paper.

2 Background

This section examines DoS/DDoS attacks, HTTP flooding DDoS attacks, and the various DDoS attack defense measures.

2.1 Botnet

Malware, flash events or flash crowds, botnets, and DoS or DDoS attacks are the most well-known network attack categories. Let's start with malware, which is the first type of attack they define. Malware is generic because of its abstract formulation, which is abstract, independent of but nevertheless generally applicable to the numerous concrete manifestations of malware. Furthermore, a Flash mob is a surge of traffic to a certain web site over a relatively short period of time that occurs during extraordinary events such as breaking news and the debut of a popular product and is created by a connection between a small site and a well-known web site [9].

Robot malware is malicious software that is installed on a computer and may be remotely controlled by the robot master to do certain activities in response to commands. Botnets are distinct from other types of malwares in that they have a command-and-control infrastructure that employs IRC, HTTP, or P2P as a C&C channel to allow bots to execute malicious commands given by the bot master, as [10].

When (bots) employ a constant attack speed to transmit packets at the fastest available speed, they can send packets to the server to provide services to the victim (constant speed attack and acceleration attack). This number is referred to as a DDoS attack [11].

2.2 Denial of Service/Distributed Denial of Service Attack

DoS and DDoS attacks continue to be a cause of annoyance for both internet service providers and their customers, see [5]. By disrupting network connectivity between users and the server, these malicious attacks try to prevent legitimate users from obtaining online services or resources, see [12]. They are often carried out by flooding the target with traffic or delivering specially engineered packets that cause the system to crash, depriving legitimate users of online services or network resources, please see [13-14].

DoS and DDoS attackers commonly target the web servers of high-profile institutions such as banking, commerce, media, government, and trade organizations. Although DoS assaults seldom result in theft or catastrophic loss of data or assets, they can impose significant costs on victims in terms of time, money, reputation, and opportunity, as [15]. The difference between DoS and DDoS attacks is the number of attack sources. A DoS attack is launched by a single attacker, whereas a DDoS attack is launched by several attackers and can be several times more damaging due to the usage of botnet-based spread attacks, see [16]. DDoS and DoS attacks seek to degrade the quality of target services or servers, or possibly to totally shut them down, as [17].

Detecting ongoing DDoS and DoS attacks is difficult for a variety of reasons, see [18-19]. To begin, the detection procedure takes place online, giving security professionals and system administrators a limited time window to notice and validate the attack, which might lead to misclassification. Second, due to the vast number of attack sources, the assault may be started by a heterogeneous device type. Third, typical network preventative procedures such as packet filtering, software parameter tuning, and rate limiting are restricted in their ability to protect critical network resources, please see [19]. Finally, because their network data is so similar, it is impossible to distinguish DDoS attacks from flash crowd occurrences. As a result, a dependable and precise solution to identify DDoS attacks on the network is required, see [20]. DDoS attacks are commonly categorized into three main categories as listed in Table 1.

Table 1: Commonly categorized threshold of DDoS attacks.

Attack Category	Description
Volumetric Attack	The main objective of this attack is to flood the target with traffic to exhaust network or hardware resources. This category includes flooding and amplification/reflection attacks.
Protocol Exploitation	This threat type aims to exploit flaws in network protocols by ingesting connection state tables produced by some network devices.
Application Layer Attack	Vulnerabilities in application layer protocols such as HTTP and SSL are taken advantage of. These attacks can also target application code that lacks secure coding techniques. They are stealthy and difficult to identify as they use genuine communications.

2.3 Distributed Denial of Service HTTP Flooding Attacks

DDoS assaults, particularly HTTP flooding attacks, frequently target the application layer, which handles user requests and transmits data to browsers. HTTP is the most often used protocol at the application layer because it allows communication between browsers and servers. An HTTP flood attack attempts to overload a web server with requests, rendering it unavailable to legitimate users. A flood of HTTP requests can be started by a single attacker or a group of attackers working together, sometimes with the help of botnets or compromised devices please see [21-22].

The "low and slow" attack is a typical tactic used in HTTP flooding attacks in which compromised requests are used to engage the target server in high-quality computations, causing it to consume many resources while being bombarded with multiple HTTP requests. These attacks may be difficult to detect because the traffic patterns they generate may appear to be legitimate user activity, making it difficult to distinguish which requests are malicious and which are not, as [23].

HTTP flooding attacks can be difficult to detect because they might be camouflaged as valid protocol connections in network traffic. HTTP flooding attacks may leverage holes in application-layer protocols such as HTTP and SSL, as well as flaws in underlying network protocols. Flooding attacks are widespread in HTTP, the most used protocol at the application layer, as [24]. Furthermore, these attacks often use the POST and discover request methods, which are extensively used for transmitting sensitive data across the Internet.

Low-speed and low-rate HTTP attack compromised requests are used to engage the victim in high-quality computations that occupy a substantial amount of the victim's resources while the victim is bombarded with a massive array of HTTP requests, see [25]. A DDoS attack using the slow HTTP protocol renders an online service unavailable, but it is difficult to detect on a network since its traffic patterns are like those of normal users, please see [26].

3 Related Work

The purpose of this section is to examine past studies, techniques, and mechanisms relevant to the suggested Bayes-entropy mechanism. Table 2 summarizes the relevant work techniques and mechanisms [27-35].

Table 2. contains a full examination of existing studies on the proposed mechanism. It investigates each study's basic principles, mathematical functions, correctness, and potential limitations. However, it found a gap in these earlier approaches because they were focused on detecting HTTP flooding DDoS attacks in traffic via probability or randomness. To address this issue, the Bayes-entropy method must be used to compute both probability and randomness in each of the arriving aggregated packets. Failure to work them together may result in regular packets being misclassified as abnormal and vice versa.

In contrast to previous studies, the proposed work does not rely on probability-based analysis alone, entropy-based analysis alone, or general machine-learning classification alone. Instead, it introduces a unified Bayes-entropy mechanism that jointly computes the probability of HTTP flooding DDoS occurrence and the randomness of packet behavior at the event-group level within aggregated traffic packets. This makes the proposed method different from earlier approaches that examined only one traffic characteristic or used separate analytical models, because the present work integrates both measures within a single mathematical detection framework to reduce misclassification between normal and attack traffic and improve detection accuracy.

Table 2. Related works to the proposed mechanism.

Ref	Main Idea	Mathematical Functions	Results	Drawbacks
[27]	Entropy paradigm for detecting DDoS anomalies; entropy value identifies HTTP flooding attacks	$p^{\beta} = (\frac{a^c}{c!})/\sum_{i=0}^{c} \frac{a^i}{i!}$ $p^{M} = (\frac{Y^{M_{total}}}{M_{total}})/\sum \frac{Y^i}{i!}$ $a = (\beta_A + \beta_N)/\beta_{total}$ $Y = M_A + M_N = \frac{\delta_{MA}}{\tau_{MA}} + \frac{\delta_{MN}}{\tau_{MN}}$	N/A	Neglected packet content; equal-sized packets may differ in content
[28]	Entropy to calculate likelihood based on total events; massive packets reduce randomness	$H(x) = \frac{1}{1-\alpha} \log_2 \sum_{i=1}^{n} P_I^{\alpha}$,	~95%	Used false alarm rate only; logical, statistical, calculus functions only
[29]	Expected value calculation for information content in messages	$ip - proto = \frac{N_{proto}}{K}$ $E(x) = -P(X_i) \log_2 P(X_i)$ $cv(X) = \frac{std(X)}{man(X)}$ $rte = \frac{U_x}{S_x}$	~96%	Focused on logical, statistical, probability functions only
[30]	Integration of Bayesian classifier and Snort for NIDS framework in cloud	Bayesian classification probabilities	N/A	Limited to cloud environment intrusion detection
[31]	Hidden Naïve Bayes (HNB) multinomial classifier for intrusion detection	$c(E) = \arg\max_{c \epsilon C} P(c) \prod_{i=1}^{n} P(a_i \| a_{hp_i}, c)$	93.72%	Applied to DoS only; used old KDD99 dataset
[32]	Six ML models: J48, Random Tree, REP Tree, Random Forest, MLP, SVM	$H(x) = \frac{1}{1-\alpha} \log_2 \sum_{i=1}^{n} P_I^{\alpha}$	~95%	Used false alarm rate (FP and TN) only
[33]	Semi-supervised weighted k-means for HTTP DDoS using CIC DDoS dataset	$H(x) = \frac{1}{1-\alpha} \log_2 \sum_{i=1}^{n} P_I^{\alpha}$	98.86%	Did not merge entropy with other mathematical functions
[34]	ML-based DoS/DDoS detection using signatures from network traffic samples	$E(x) = -P(X_i) \log_2 P(X_i)$ $cv(X) = \frac{std(X)}{man(X)}$,	~96%	Focused on logical, statistical, probability functions only
[35]	Multi-modal probability distribution for DDoS detection at flow level	$W_m = \sum_{f=1}^{F} \overrightarrow{\mu_{b_f}} \Pr\left(\overrightarrow{\mu_{b_f}}\right)$ $\Pr\left(\overrightarrow{\mu_{b_f}}\right) = \frac{\overrightarrow{O_{b_f}}}{\sum_{f=1}^{F} \overrightarrow{O_{b_f}}}$,	~97%	Depended on correctly detecting normal and misclassification rates

4 Proposed Mechanism

To meet the research aims, this section provides Bayes-entropy, a mathematical-based approach for identifying HTTP flooding attacks. The suggested method detects DDoS assaults based on HTTP traffic by watching the characteristics of aggregated packets acquired from network traffic within a given time (t). Figure 1 depicts the four phases of the proposed mechanism.

The general phases of this mechanism to prepare the captured packets from the traffic are: (i) data pre-processing, (ii) packets aggregated attributes, (iii) anomaly-based detection and (iv) rule based.

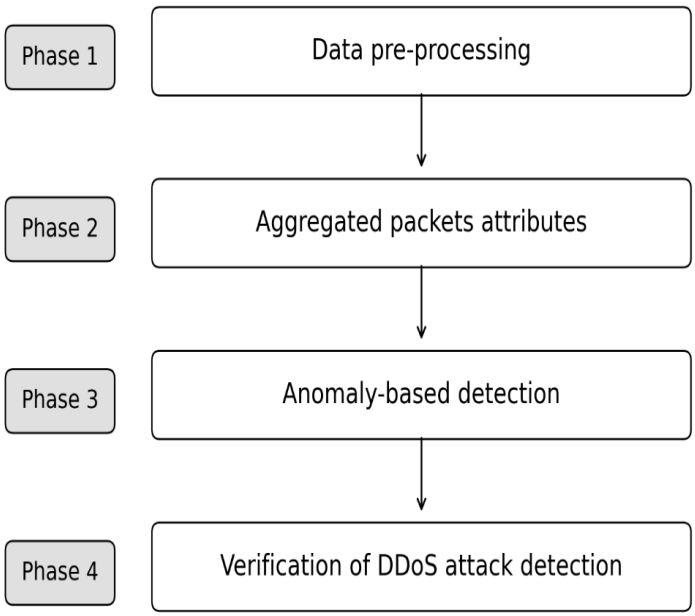


Fig. 1 Methodology of the proopsed mechanism.

4.1 Data pre-processing

This step receives the collected packets, filters them for HTTP packets, and then cleans the data to remove duplicates. This procedure is divided into two stages: data filtration using Wireshark filtering commands to exclude non-HTTP packets that are outside the scope of the research, and data cleansing up using SQL statements to remove redundant packets, which are then used as inputs for the next phase (aggregated packet attributes), as [36].

4.1.1 Data filtration

Not all inbound and outbound network packets are connected and contribute to the detection of HTTP flooding DDoS attacks. As a result, instead of monitoring or observing the complete network traffic, just HTTP activity should be monitored or observed. This decreases the proposed approach's resource overhead. The initial stage is to filter incoming network data

to only include HTTP traffic, and then extract specific information from the HTTP header. Source IP, destination IP, and packet size are among the extracted features. These traits were chosen based on HTTP traffic experiments and observations, and they are known to aid in the identification of HTTP flooding DDoS attacks. Other scholars, such as [35, 37-38], have also employed these qualities in their studies.

4.1.2 Data Cleansing

The data cleansing procedure entails locating and repairing flaws in the data set as well as removing conflicting occurrences. Furthermore, cleaning up the data can increase the accuracy of the results while reducing the time spent searching for records [39-40]. Furthermore, the data cleansing procedure restores lost values inside datasets, explains the values of outliers, and corrects any contradictions. After the data filtering and purification phases are completed, the packets will be used as inputs in the next phase (aggregated packets attributes).

4.2 Aggregated Packets Attributes

The suggested mechanism's second phase aggregates the captured packets every (t) second. Based on time (t), the aggregated packets in each (groupni) will be further divided into x events. The packets will be grouped (groupyij) for each (groupxi) based on three attributes: the number of packets, the size of packets, and the regularity of inter-arrival time of packets. Because this mechanism is based on events and their values, the purpose for breaking the aggregated packets into events is to prepare them as input of (summation rows-columns) in the following step. The number of events (x) in each (groupni) is determined by the experimental and observational results of the HTTP flooding.

4.2.1 Equal Packets Size

The first attribute aims to monitor the size of the HTTP packets in eventxij to help the proposed approach detect HTTP flooding DDoS attacks in each eventxij by observing the packets sizes. It appears that most HTTP flooding DDoS attacks tend to send a myriad of same-sized HTTP packets to the targeted server with deliberate intent to make it unavailable/unresponsive to legitimate users. So, the proposed approach classifies the incoming HTTP packets in the eventxij according to their size. The output of this stage is to put the incoming packets in groups according to their size in the (n) group, where n represents the number of distinct packet sizes.

4.2.2 Regularity of Packets Inter-Arrival

The second attribute aims to observe the regularity of the packets' inter-arrival time in each eventxij from the previous step through computing the inter-arrival time between each adjacent packet. These adjacent packets must be equal in size. The inter-arrival time between any two adjacent packets of the same packet size may be different or equal in the groupyij of eventxij. If inter-arrival time is different, this mechanism will consider this eventxij has normal packets; otherwise, eventxij has HTTP DDoS attacks, which is the main goal of this research.

In normal HTTP requests, users usually send HTTP packets, i.e., by browsing a particular website, and these requests result in different packet sizes and inter-arrival times. However, unlike the HTTP flooding DDoS attacks, the hackers tend to deprive the services of the legitimate users by sending countless HTTP packets with similar packet sizes and the exact inter-arrival times. Therefore, the number of the incoming HTTP packets in the groupyij is essential for the anomaly-based detection phase in the proposed detection mechanism to detect HTTP DDoS attacks.

4.2.3 Number of Packets

The third attribute observes and counts the number of all HTTP packets in each eventxij of the aggregated packets groups (groupni). The number of the HTTP packets with the same size and the exact interval time in each groupyij of eventxij is considered the third attribute of the aggregated packets attributes phase. There is a direct correlation between the number of HTTP packets in groupyij of eventxij and the occurrence of HTTP flooding DDoS attacks inside this eventxi.j. Therefore, if the groupyij has many HTTP packets with the same packet size and interval time, it could be a clue for HTTP flooding DDoS attacks.

In summary, the aggregated packets groupn with (t) time are further split into (x) events, and each eventxij is divided into groupyij according to equal packets size, (ii) regularity of the packets inter-arrival time, and (iii) number of packets. If any eventxij exhibits any abnormality, the aggregated packets groupn will be considered HTTP flooding attacks based on the next phase. The three attributes will be used as inputs for the next phase (anomaly-based detection) to detect the presence of HTTP DDoS attacks in the aggregated packets (groupyij).

4.3 Anomaly-Based Detection

The third step uses the proposed indicator (Bayes-entropy) to detect the aberrant HTTP DDoS assault within each aggregated packet. The proposed indicator (Bayes-entropy) is regarded as the central component of an anomaly-based phase. The aggregated packets from the previous phase are used as inputs in groupyij to determine the probability and randomness of HTTP packets using three attributes: packet size, regularity, and number of packets. Using Bayes-entropy functions, it attempts to classify the groupyij of each event in the aggregated packet (groupn) as normal, suspicious, or HTTP flooding DDoS attack.

The strength of this indicator (Bayes-entropy) lies in its ability to combine the Bayes theorem and the entropy equation to detect abnormal behavior of HTTP packets in each event in the aggregated packets captured from the traffic. It works by working together on groupyij for each eventxj to compute its probability of DDoS using Bayes and its randomness using the entropy equation. Thus, this indicator will work on the event level.

The Bayes theorem or entropy will produce many false positives when used to identify HTTP DDoS attacks. As a result, this indicator argues that applying the Bayes theory and entropy to the groupyij of each event in the aggregated packet will increase detection accuracy and reduce the false-positive rate of HTTP DDoS attacks. The probability value of the Bayes theory does not ensure the occurrence of an HTTP DDoS attack. As a result, calculating the

probability of an HTTP DDoS assault and assessing the randomness of HTTP traffic will increase the assurance of its presence, see [33].

The proposed mechanism works according to the following steps:

1. Every 60 seconds, this indicator aggregates traffic into packets, separates each aggregated packet into 5-second events, and divides each event into groups based on packet size and inter-arrival time. It then computes the Bayes and entropy values for each event; because the aggregated packets contain numerous events, the proposed indicator uses the (OR operation) to extract the result of each event in the aggregated packet.
2. It computes the probability of each event using Eq. 1.

$$\mathrm{P(event)} = \mathrm{P(E_i)} = \frac{1}{\#\text{ number of the events in the aggregated packets}} = \frac{1}{12} \quad (1)$$

Note: Each event is equal to 5 seconds and the total time for the aggregated packets is 60. Thus, the total number of events in aggregated packets is 12 events (60/5).

3. This indicator calculates for each event:

(a) Divide the packets into equal-sized groups with the same inter-arrival time.

(b) The probability of HTTP flooding DDoS attacks occurring using Eq. 2.

$$P(\mathrm{DDoS}) = \sum \mathrm{P(E_i)}.\,\mathrm{P(DDoS|E_i)} = \frac{\#\text{ of packet size with equal inter arrival in the } \mathrm{E_i}}{\#\text{ of total packets in this } \mathrm{E_i}}$$

$$= \frac{1}{12}\left(\frac{\#\text{ of packets in } \mathrm{G_1}}{\#\text{ packets in } \mathrm{E_1}} \cdot \frac{\#\text{ of packets in } \mathrm{G_2}}{\#\text{ packets in } \mathrm{E_1}} + \frac{\#\text{ of packets in } \mathrm{G_1}}{\#\text{ packets in } \mathrm{E_2}} \cdot \frac{\#\text{ of packets in } \mathrm{G_2}}{\#\text{ packets in } \mathrm{E_2}} + \cdots \right) \quad (2)$$

(c) The probability of an event occurring in the presence of DDoS using Bayes theorem see Eq. 3.

$$P(\mathrm{E_i|DDoS}) = \frac{\mathrm{P(E_i \cap DDoS)}}{\mathrm{P(DDoS)}} = \frac{\mathrm{P(E_i)}\,.\,\mathrm{P(DDoS|E_i)}}{\sum \mathrm{P(E_i)}.\,\mathrm{P(DDoS|E_i)}}$$

$$= \frac{\frac{\#\text{ of packet size with equal inter arrival time in } \mathrm{E_i}}{12\,.\,\#\text{ total packets in the } \mathrm{E_i}}}{\mathrm{P(DDoS)}} \quad (3)$$

(d) The randomness of the event using entropy see Eq. 4.

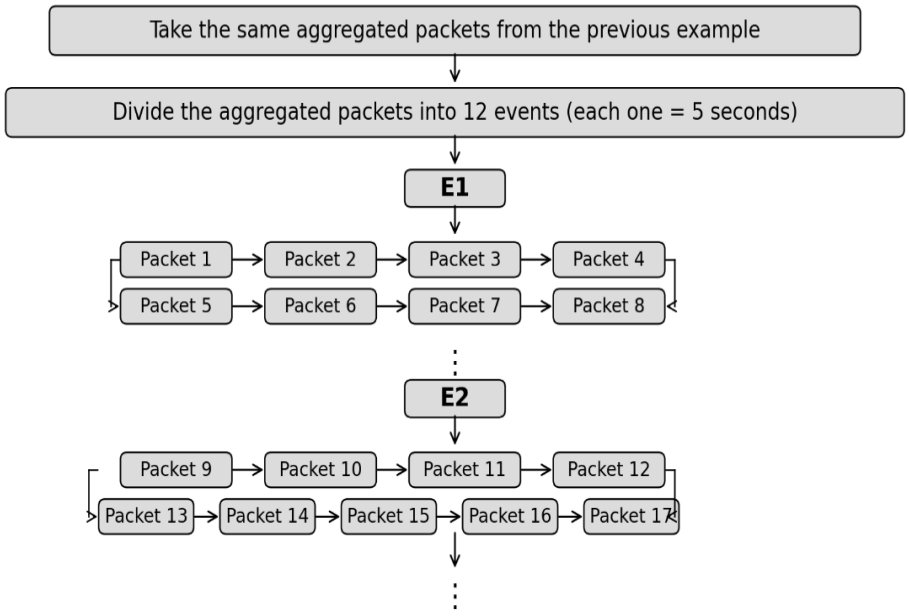
$$\mathrm{H(x)} = -\sum \mathrm{P(E_i/DDoS)}.\log_{\mathrm{E}} \mathrm{P(E_i/DDoS)} \quad (4)$$

The Bayes theorem is used to calculate the probability of an HTTP DDoS attack, and the entropy function is used to measure the unpredictability of the packets. If ($\alpha_1 \leq$ the Bayes value of the groups ≤ 1 and $0 \leq$ the entropy value of this group $\leq \alpha_2$), then groupyij is HTTP DDoS attack; meanwhile, if ($0 \leq$ the Bayes value of the group $\leq \alpha_3$ and $\alpha_4 \leq$ the entropy value ≤ 1), then it is normal; otherwise, it is suspicious.

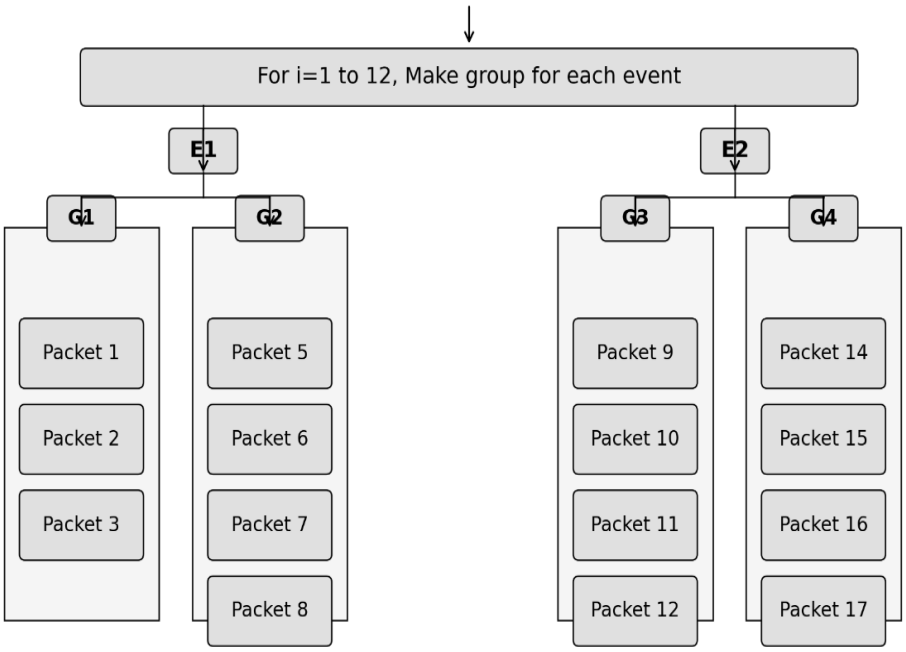
The values α_1, α_2, α_3 and α_4 is determined based on probability science. So, the threshold values of the proposed mechanism are (α_1=0.75, α_2=0.25, α_3=0.25 and α_4=0.75) and the justification of them are summarized in the Table 3. as followed:

Table 3: The threshold of the indicator.

Parameter	**Value**	**Region/Justification**
α_1	0.75	Close to 1 region (DDoS) based on three proportional regions (1:2:1) [42]
α_2	0.25	Close to 0 region (DDoS for entropy)
α_3	0.25	Close to 0 region (Normal for Bayes)
α_4	0.75	Close to 1 region (Normal for entropy)



(A)



(B)

Fig. 2 Input network traffic.

4.4 Rule Based DDoS Attack Detection

Based on the following principles, this phase seeks to categorize the aggregated packets as either regular, suspicious, or HTTP flooding DDoS:

Rule 1: If $(0 \leq H(x) \leq 0.25 \wedge 0.75 \leq P(DDoS) \leq 1)$ Then: Output: HTTP flooding DDoS attack. Else if $(0.75 \leq H(x) \leq 1 \wedge 0 \leq P(DDoS) \leq 0.25)$ Then: Output: normal. Else: Output: suspicious.

Rule 2: The decision equation collects the group's results then applies an (OR) operation to label the event of the aggregated packets as either DDoS (result = 1), normal (result = 0), or suspicious (result = neglect). Decision equation = ($result_1$ OR $result_2$ OR ... OR result k)

Rule 3: If the result of the decision equation is 1, the proposed approach considers the aggregated packets as HTTP flooding attack.

5 Illustrative Example

This section provides an illustrative example of the suggested mechanism for detecting DDoS HTTP flooding assaults in network traffic. Figure 2depicts the input network traffic before explaining how the technique will operate.

Then, the proposed mechanism will compute the probability for each event as: P(Ei) = 1/n = 1/12, where n is the number of events (each representing a 5 second time window).

Then it will compute the probability of DDoS in this event, the probability of Ei when the DDoS already occurred using Bayes theorem, and the randomness using entropy. The example calculation shows P(DDoS) = 0.0308, P(Ei|DDoS) = 2.3701, and H(x) = 11.90.

Then it will apply rule #1 and rule #2 on E1. As a result, event 1 (E1), is suspicious based on the condition mentioned above. Then, the decision equation collects the rest event's results, applies (OR) operation, and then labels this event of the aggregated packets as DDoS attack and the output = 1; if one event classified as DDoS attacks then the whole aggregated packet considered as DDoS attack.

6 Experimental Results

This section introduces the dataset as well as the evaluation criteria that will be utilized to apply the suggested technique and subsequently extract its correctness.

6.1 Dataset

This paper uses ISCX dataset (unb.ca/cic/datasets/ids.html) to apply the proposed mechanism on it. It was collected from the University of New Brunswick and is made up of collections of numerous publicly available non-malicious and malicious datasets totaling 393 MB. It also includes HTTP DDOS assault packets, and both datasets employ a PCAP file. The most frequent dataset forms utilized in DDOS attack detection techniques are CSV and PCAP, see [41]. The ISCX dataset contains four separate attack types: Brute Force, SSH, Infiltrating, HTTP DoS, and DDoS, logged alongside normal traffic on seven consecutive days, as [32]. This dataset also includes HTTP DDoS traffic, as shown in Table 4.

Table 4. Summary of ISCX dataset

Attribute	Value
Dataset type	Multi-class
Year of formation	2012
Duration of Capture	Seven days
Features	20
Number of Classes	2
Number of packets	695,052
Number of normal packets	681,151
Number of malicious packets	13,901

6.2 Evaluation Metrics

The evaluation metrics (TP, TN, FP, and FN) are presented in this section. The proposed method employs quantitative criteria to assess the proposed approach's accuracy in identifying HTTP flooding DDoS attacks on web servers. True-positive (TP) indicates accurately classified harmful traffic, and true-negative (TN) indicates correctly classified normal traffic. Furthermore, false-positive (FP) traffic is misclassified hostile traffic, whereas false-negative (FN) traffic is misclassified regular traffic [42-43]. The quantitative metrics utilized in this paper are listed in Table 5. Detection accuracy (AC) = (TP + TN)/(TP + FP + FN + TN) × 100

Table 5: Evaluation metrics (confusion matrix)

	Malicious traffic	**Normal traffic**
Malicious traffic	True-negative (TN)	False-positive (FP)
Normal traffic	False-negative (FN)	True-positive (TP)

The following equations are used in this study to evaluate the evaluation metrics and the accuracy of the suggested approach.

$$\text{True Positives} = \frac{TP}{TP+FN} \quad (5)$$

$$\text{True Negative} = \frac{TN}{TN+FP} \quad (6)$$

$$\text{False Positives} = \frac{FP}{TN+FP} \quad (7)$$

$$\text{False Negative} = \frac{FN}{FN+TP} \quad (8)$$

$$\text{Detection accuracy (AC)} = \frac{\text{TP+TN}}{\text{TP+FP+FN+TN}} \times 100 \quad (9)$$

6.3 Result and Discussion

This section tries to assess the suggested mechanism's capacity to identify HTTP flooding DDoS attacks accurately. The assessment is primarily concerned with estimating the detection accuracy. The threshold (t), which indicates the aggregated packets' time slot, is determined. (t) = 60 seconds in this experiment; the choice of (t) is based on earlier research, such as [33] and [36]. The ISCX dataset was divided into 35 aggregated packets, where each represents a 60-second time slot. Therefore, a total of 2,100 (35 x 60) seconds of HTTP traffic is used in this experiment. Table 6 shows a sample of HTTP packets in each group.

Table 6: ISCX dataset groups

Attribute	Value
Size	393 MB
Number of packets	695,052
Number of the aggregated packets	35
Number of the groups of aggregated packets	420 (12×35)

By applying the proposed mechanism on the 420 events of the ISCX dataset reveals the quantitative metrics: the true-positive rate is (13 ≡ 92.85%), the false-negative rate is (1 ≡ 7.14%), the false-positive rate is (0 ≡ 0%), and the true-negative rate is (21 ≡ 100%). Therefore, the detection accuracy rate of the proposed mechanism, calculated using Eq. 9, is 97.14%. Figure 3 shows the quantitative metrics analysis on the ISCX dataset.

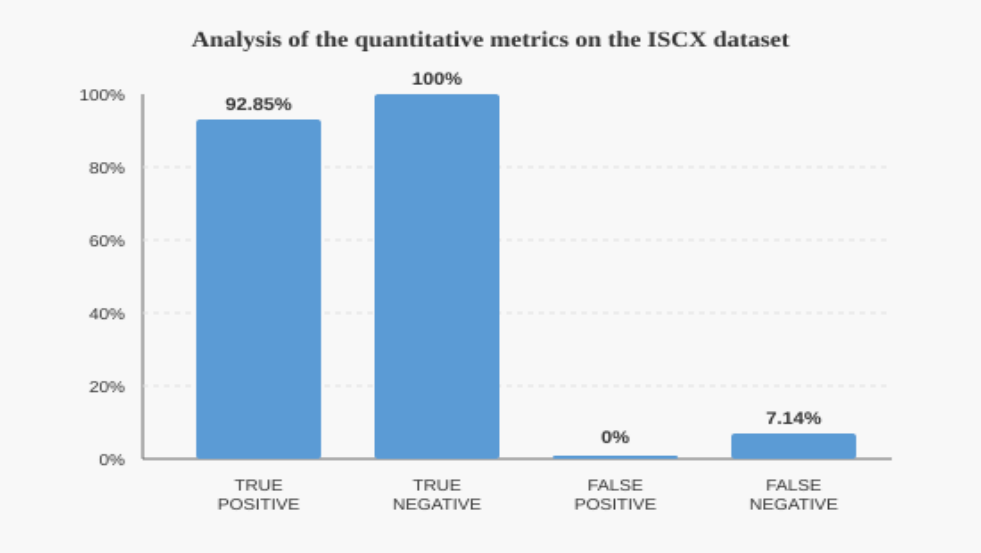


Fig. 3 Analysis of the proposed mechanism on the ISCX dataset.

To better understand the provided results, the proposed technique was implemented on a sample of packets from the ISCX dataset to compute detection accuracy. This sample is 300 seconds long, and the findings are shown in Table 7.

Table 7: Implementing the proposed indicator on the ISCX dataset (summarized)

Aggregated Packet	Original Label	Events Classified (True)	Voting Result	Final Result
Packet 1	Normal	E_9, E_{11} (2/12)	Normal	**TP**
Packet 2	Normal	E_8, E_{10}, E_{12} (3/12)	DDoS	**TN**
Packet 3	Normal	E_{10} (1/12)	Normal	**TP**
Packet 4	Normal	E_1, E_8, E_{12} (3/12)	Normal	**TP**

Aggregated Packet	Original Label	Events Classified (True)	Voting Result	Final Result
Packet 5	DDoS	E_1, E_{10} (2/12)	DDoS	**FN**

The proposed mechanism (Bayes-entropy) computes the values of Bayes and entropy for each groupyij of each eventxi. Some events were misclassified due to the values of (Bayes and entropy) not matching the thresholds α_1=0.75 and α_2=0.25. However, this mechanism still demonstrates strength in detecting misbehaviors in the aggregated packets due to the small number of misclassification cases. Based on Table 7, the detection accuracy (AC) = (3+1)/(3+1+1+0) = 4/5 = 80% for this sample.

The fourth section compares the proposed mechanism's detection accuracy rate in detecting HTTP flooding DDoS attacks with a statistical method-based machine learning DoS/DDoS detection system, as [34] and a statistical method-based multi-modal probability distribution to detect DDoS attacks [35]. Table 8 shows the outcome of the comparison using the ISCX dataset for each mechanism.

Table 8: Comparison of accuracy rates with existing mechanisms

DDoS Detection Mechanism	Accuracy Rate
[34] ML-based DoS/DDoS detection	96%
[35] Multi-modal probability distribution	97%
Proposed Bayes-Entropy Mechanism	**97.14%**

Table 8 shows that the detection accuracy rate of the proposed mechanism is higher than the comparative approaches, please see [34-35], indicating that the main hypothesis of this paper is correct; to improve the detection accuracy rate of existing detection mechanisms by applying both Bayes and entropy functions to captured packets in the aggregated packet from traffic

7 Conclusion

This research described a mathematical approach for detecting HTTP flooding DDoS assaults. The suggested mechanism computes Bayes-entropy functions for each interval group in the aggregated traffic packet. The experimental evaluation on the ISCX dataset showed that the proposed mechanism achieved a detection accuracy of 97.14%, with a true-positive rate of 92.85%, a true-negative rate of 100%, a false-negative rate of 7.14%, and a false-positive rate of 0%. In addition, the proposed Bayes-entropy mechanism outperformed the comparative methods reported in the literature, which achieved accuracy rates of 96% and 97%, respectively. For the first time, this work uses the Bayes theorem and the entropy equation to detect abnormal HTTP packet behavior, increasing the efficiency of the incoming mechanisms; the

greater the use, the greater the efficiency, and vice versa. Several experiments were carried out to calibrate and evaluate the system's performance. The results demonstrated that the proposed strategy is viable and performs better than several current and relevant approaches available in the literature. When applied to the ISCX dataset, this work can discriminate between routine, suspicious, and flooding HTTP DDoS attacks in the traffic and reach accuracy rates of 97.14%.

This study has some limitations that should be acknowledged. First, the proposed Bayes-entropy mechanism is designed specifically for detecting HTTP flooding DDoS attacks on web servers, which limits its direct applicability to other attack types or application-layer protocols. Second, the experimental validation was conducted using the ISCX dataset only, and broader evaluation on additional datasets is still needed to further confirm the generalization ability of the proposed method. Third, the mechanism relies on arriving aggregated network packets rather than web server access logs, which may restrict its effectiveness in environments where packet-level traffic capture is limited or unavailable.

Future work will extend the proposed Bayes-entropy mechanism in several specific directions. First, the method will be evaluated on additional and more recent benchmark datasets to examine its generalization ability beyond the ISCX dataset. Second, the current framework will be expanded to detect other application-layer flooding attacks, particularly those targeting protocols such as DNS, MQTT, XMPP, and CoAP. Third, future studies will investigate adaptive threshold selection instead of using fixed threshold values, in order to improve robustness under dynamic traffic conditions. Fourth, the proposed mechanism will be tested using web server access logs in addition to aggregated network packets to compare detection effectiveness across different data sources. Finally, the integration of the Bayes-entropy mechanism with real-time network monitoring and security management platforms will be explored to support practical deployment in operational environments.

References

[1] Shehab, M., Shambour, M. K. Y., Abu Hashem, M. A., Al Hamad, H. A., Shannaq, F., Mizher, M., Jaradat, G., Daoud, M. Sh., & Abualigah, L. (2024). A survey and recent advances in black widow optimization: Variants and applications. *Neural Computing and Applications*, 1–21.

[2] Nagm, A. M., Gomaa, M., Sbera, R., El-Douh, A. A., Abdelhafeez, A., & Fakhry, A. E. (2025). Neutrosophic set and machine learning models for detection of DoS attack resilience. *Neutrosophic Sets and Systems*, 87, 352–361.

[3] Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: Classification and art. *International Journal of Computer Applications*, 49(7), 24–32.

[4] Park, K., & Lee, H. (2001). On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. *ACM SIGCOMM Computer Communication Review*, 31(4), 15–26.

[5] Tayyab, M., Belaton, B., & Anbar, M. (2020). ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review. *IEEE Access*, 8, 170529–170547.

[6] Bhuyan, M. H., Kashyap, H. J., Bhattacharyya, D. K., & Kalita, J. K. (2013). Detecting distributed denial of service attacks: Methods, tools, and future directions. *The Computer Journal*, 57(4), 537–556.

[7] Al Ghamri, M., Ibrahim, D., Sihwail, R., & Shehab, M. (2025). Whale optimization algorithm for feature selection enhances classification in malware datasets. *Journal of Computational and Cognitive Engineering*, 4(3), 387–396.

[8] Shehab, M., Tarawneh, O., AbuSalem, H., Shannag, F., & Al-Omari, W. (2022). Improved gradient-based optimizer for solving real-world engineering problems. *In 2022 4th IEEE Middle East and North Africa Communications Conference (MENACOMM)* (pp. 191–196). IEEE.

[9] Pai, V. S., Druschel, P., & Zwaenepoel, W. (1999). Flash: An efficient and portable web server. *In USENIX Annual Technical Conference*. USENIX.

[10] Barford, P., & Yegneswaran, V. (2007). An inside look at botnets. *In Malware Detection. Springer*.

[11] Thapngam, T., Yu, S., Zhou, W., & Beliakov, G. (2011). Discriminating DDoS attack traffic from flash crowd through packet arrival patterns. *In International Workshop on Security in Computers, Networking and Communications*.

[12] Bahashwan, A. A., Anbar, M., & Hanshi, S. M. (2020). Overview of IPv6 based DDoS and DoS attacks detection mechanisms. *Springer, 1132*.

[13] Yan, Q., & Yu, F. (2015). Distributed denial of service attacks in software-defined networking with cloud computing. *IEEE Communications Magazine*, 53(4), 52–59.

[14] Jalili, R., Imani-Mehr, F., Amini, M., & Shahriari, H. R. (2005). Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks. *In International Conference on Information Security Practice and Experience (ISPEC)* (Vol. 3439, pp. 192–203).

[15] Darwish, M., Ouda, A., & Capretz, L. F. (2013). Cloud-based DDoS attacks and defenses. *In International Conference on Information Society (i-Soc)* (pp. 67–71).

[16] Elejla, O. E., Anbar, M., & Belaton, B. (2017). ICMPv6-based DoS and DDoS attacks and defense mechanisms: Review. *IETE Technical Review*, 34(4), 390–407.

[17] Balarezo, J. F., Wang, S., Chavez, G., Sithamparanathan, K., Kandeepan, S., & Al-Hourani, A. (2022). A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. *Engineering Science and Technology, an International Journal*, 31.

[18] Jin, S., & Yeung, D. S. (2004). A covariance analysis model for DDoS attack detection. *In IEEE International Conference on Communications* (pp. 1882–1886). IEEE.

[19] Elejla, O. E., Anbar, M., Belaton, B., & Alijla, B. O. (2018). Flow-based IDS for ICMPv6-based DDoS attacks detection. *Arabian Journal for Science and Engineering*, 43(12), 7757–7775.

[20] Elejla, O. E., Belaton, B., Anbar, M., Alabsi, B., & Al-Ani, A. K. (2018). Comparison of classification algorithms on ICMPv6-based DDoS attacks detection. *In Computational Science and Technology* (Vol. 481, pp. 347–357). Springer.

[21] Ghaben, A., Anbar, M., Hasabullah, I. H., & Karuppayah, S. (2021). Mathematical approach as qualitative metrics of distributed denial of service attack detection mechanisms. IEEE Access.

[22] Jaafar, A., Abdullah, M., & Ismail, R. (2019). Review of recent detection methods for HTTP DDoS attack. *Journal of Computer Networks and Communications*, 2019.

[23] Lrt, J., Beng, L. Y., Park, Y., & Anbar, M. (2022). Capturing collusive interest flooding attacks signal: A novel Malaysia's state named-data networking topology (MY-NDN). *Journal of Engineering Science and Technology*, 17, 997–1009.

[24] Singh, K., Singh, P., & Kumar, S. (2017). Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. *Computers & Security*, 65, 344–372.

[25] Afdel, K., & Belouch, M. (2018). Semi-supervised machine learning approach for DDoS detection. *Applied Intelligence*.

[26] Hong, K., Kim, Y., Choi, H., & Park, J. (2018). SDN-assisted slow HTTP DDoS attack defense method. *IEEE Communications Letters*, 22(4).

[27] Wang, X., Jia, Y., & Ju, F. (2015). Separation and enrichment of PbS and Sb2S3 from jamesonite by vacuum distillation. *Vacuum*, 121, 48–55.

[28] Mousavi, S. M., & St-Hilaire, M. (2015). Early detection of DDoS attacks against SDN controllers. *In International Conference on Computing, Networking and Communications.*

[29] Khan, A., Gani, A., Wahid, A., Wahab, A., & Singh, R. (2017). Feature selection of denial-of-service attacks using entropy and granular computing. *King Fahd University of Petroleum & Minerals*.

[30] Modi, C. N., Patel, D. R., Patel, A., & Rajarajan, M. (2012). Bayesian classifier and Snort based network intrusion detection system in cloud computing. In International Conference on Computing, *Communication and Networking Technologies (ICCCNT)*.

[31] Koc, L., Mazzuchi, T. A., & Sarkani, S. (2012). A network intrusion detection system based on a hidden naïve Bayes multiclass classifier. Expert Systems with Applications, 39(18), 13492–13500.

[32] Soheily-Khah, S., Marteau, P. F., & Bechet, N. (2018). Intrusion detection in network systems through hybrid supervised and unsupervised machine learning process: A case study on the ISCX dataset. *In International Conference on Data Intelligence and Security (ICDIS)*.

[33] Mohammad, A., Mohammed, A., Iznan, H. H., & Yw, C. (2021). Entropy-based approach to detect DDoS attacks on software defined networking controller. *Computers, Materials & Continua*, 69(1), 373–391.

[34] Lima Filho, F. S., et al. (2019). Smart detection: An online approach for DoS/DDoS attack detection using machine learning. *Security and Communication Networks*.

[35] Ejaz, A. M., Ullah, S., & Kim, H. (2019). Statistical application fingerprinting for DDoS attack mitigation. IEEE Transactions on Information Forensics and Security, 14(6), 1471–1484.

[36] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39–53.

[37] Luo, H., Gu, Y., Liao, X., Lai, S., & Jiang, W. (2019). Bag of tricks and a strong baseline for deep person re-identification. *IEEE Xplore*.

[38] Perez-Diaz, J. A., Valdovinos, I. A., Choo, K. K. R., & Zhu, D. (2020). A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, 8, 155859–155872.

[39] Liu, H., & Motoda, H. (2001). Data reduction via instance selection. *The Springer International Series in Engineering and Computer Science (SECS)*, 608.

[40] Gogoi, P., Bhattacharyya, D. K., Borah, B., & Kalita, J. K. (2011). A survey of outlier detection methods in network anomaly identification. *The Computer Journal*, 54(4), 570–588.

[41] Malik, J., et al. (2020). Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in SDN. *IEEE Access*, 8, 134695–134706.

[42] Li, M., & Li, M. (2009). A new approach for detecting DDoS attacks based on wavelet analysis. *In International Congress on Image and Signal Processing* (pp. 1–5). (Publisher not specified).

[43] Purwanto, Y., & Rahardjo, B. (2014). Traffic anomaly detection in DDoS flooding attack. *In International Conference on Telecommunication Systems, Services and Applications (TSSA)* (pp. 1–6).