

Detection and mitigation of DDoS attacks in internet of things using a fog computing hybrid approach

Karrar Falih Hassan, Mehdi Ebady Manaa

Department of Information Networks, College of IT, University of Babylon, Babylon, Iraq

Article Info

Article history:

Received Jan 22, 2022

Revised Apr 19, 2022

Accepted May 17, 2022

Keywords:

DDoS attack
Fog computing
IoT
KNN algorithm
Real time

ABSTRACT

The introduction of a new technology has aided the exponential growth of the internet of things (IoT), allowing for the connecting of more devices in the IoT network to be made possible by the availability of quicker connections and reduced latency. As IoT networks have become more prevalent and widely used, security has become one of the fundamental requirements, and a distributed denial of service (DDoS) attack poses a significant security threat due to the limited resources (CPU, memory, open source, persistent connection) that can be used to either intentionally or unintentionally increase DDoS attacks. Fog computing is proposed in this study as a framework for real-time detection and mitigation of DDoS assaults. Fog computing is accurate and quick in detecting attacks due to its proximity to IoT devices. DDoS assaults are detected using an approach that combines randomness measurement of traffic with k-nearest neighbors (KNN) machine learning algorithm. Suggested system obtained 100% detection accuracy for transmission control protocol TCP attacks, 98.79% detection accuracy for UDP attacks, and 100% detection accuracy for internet control message protocol ICMP attacks.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Karrar Falih Hassan

Department of Information Networks, College of IT, University of Babylon

Babylon, Iraq

Email: Karrar.alhashimi22@gmail.com

1. INTRODUCTION

As technology advances, devices get smaller and less costly, not to mention the widespread acceptance of the always-connected notion in today's networks, the world is becoming more linked. This innovation makes it possible for all devices to connect with one another without difficulty, establishing the framework for the Internet's future. The internet of things (IoT) is a new concept for the future of the Internet that is still in its early stages. IoT stands for the IoT, which is a network of interconnected objects and services that can communicate and collaborate with one another by utilizing the Internet as a communications system. Examples of IoT devices include thermal imaging devices, laser scanners, gas indicators, and global positioning systems, among others [1].

Improved communication technologies such as 5G, as well as the low cost and high density of sensing devices, have all contributed to the expansion of the IoT. IoT applications have the potential to dramatically improve people's lives, including how they live, work, study, and have fun. For example, smart homes, smart health, smart cities, smart agriculture, and other industries may offer occupants a variety of benefits. More items will be linked at a faster rate and with lower latencies as a result of the 5G network, which will improve the efficiency of delay-sensitive IoT applications [2].

In order to analyze and store data in centralized computing, most IoT devices have limited resources (CPU, memory, open source, and permanent connection) and thus must be sent via the internet. This is how IoT devices analyze data in order to extract essential information that can then be securely stored in the cloud. With the proliferation of IoT devices, the amount of data has expanded, resulting in the need for a strong processing engine. In order to get to cloud computing, this vast amount of data must first go via the IoT networks, which generates substantial congestion. Eventually, the concept of fog computing arose, which processes data close to the devices and stores it locally in order to reduce overall data flow to the cloud while maintaining high-quality service and giving a speedy, real-time response to applications that demand it [3], [4].

When used in conjunction with IoT devices, fog computing can help to alleviate the limitations imposed on the devices by their need for high computing power due to the large amount of data they generate. Data can be sent to the cloud for storage, and the fog layer acts as an intermediary layer between the IoT network and the cloud layer, allowing for a faster response rate than what was previously available in the cloud as shown in Figure 1. Because of the fog of computing, it necessitates a continuous internet connection, making it vulnerable to various types of attacks, such as distributed denial of service (DDoS), which is one of the most serious types of attacks, in which a large number of requests are made to a server until it stops responding or becomes inaccessible, and which is one of the most serious types of attacks [5]. Providing for the safety and preservation of the environment the fact that the data being processed is so sensitive and pertains to the lives of the general public, and such as fire alarms, makes it impossible to avoid this practice. When a DDoS attack is launched, the goal is to overburden computer resources, services, or networks to the point that they become inaccessible or incapable of fulfilling their main purpose. Because such cyber-attacks prevent authorized customers from accessing the service (for example, accessing an email account, other bank or other accounts, or visiting a website), they are referred to as undesirable services. The most common form of such undesirable services is access to the Web server, which is intended for use on a website [6].

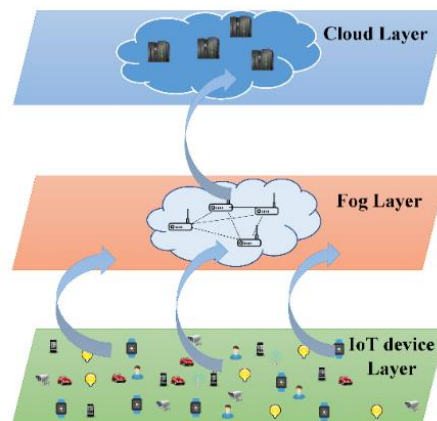


Figure 1. IoT architecture in cloud and fog computing

The existence of numerous devices connected to the Internet that launch a DDoS attack at the same time in order to interrupt the services that the server provides to customers is referred to as DDoS. Although DDoS attacks are widespread throughout the world, there are currently no preventive measures in place to mitigate or mitigate the risk of being targeted by one, which are considered insufficient despite their widespread nature. The history of DDoS attacks has shown that the number of attacks has increased significantly over time, as has the diversity of attacks and the average number of attacks per day [7]. DDoS attacks are becoming more common. An attacker floods the target server with data packets from network computers to the point that it is unable to receive or reply to data packets, resulting in the system being forced to shut down. However, a significant delay is sufficient to make the system unworkable as a result of the increased reaction time [8]. Zombie computers are infected computers that may be operated remotely without the user's knowledge or consent. It is constructed from the term's "robot" and "network," and it refers to a network of bots that is comprised of many different bots, collectively known as a botnet. Infected devices, bot owners, or a group of bot controllers may be assigned duties by an infected application called a bot controller.

The Mirai DDoS assault in 2016 is one of the most well-known DDOS attacks. Attackers employ a set of devices known as zombies to launch DDoS assaults, infecting a large number of devices around the globe. In October of the same year, the world experienced the largest DDoS assault, at 1.2 gigabytes per second. Because of the nature of the Internet, which is meant to provide services rather than provide protection, DDoS

assaults are very effective, yet the Internet is supposed to provide users with security and services. Attackers exploited the widespread use of IoT devices, as well as their lack of protection and maintenance, to launch DDoS attacks and gain control over a large group of people to carry out large and dangerous attacks, resulting in the IoT revolution being limited in its negative aspects and keeping the positive aspects contained [9].

2. RELATED WORKS

Using online sequential extreme learning machines, Prabavathy *et al.* [10] presented a detection system based on fog computing and online sequential extreme learning machines (OS-ELM). This system is capable of dealing with large amounts of data flow in order to identify assaults in a timely manner. The system's work has been separated into two levels: the first level is responsible for detecting attacks in fog computing, after which it transmits the information to a cloud server, and the second level is responsible for assessing the security condition of IoT devices. The model was evaluated on a data set (NSL-KDD), which yielded excellent results in terms of the detection rate of assaults in fog computing, with a detection rate of 97.36% achieving high accuracy. However, when comparing the detection rates for fog computing with cloud servers, the researchers found that fog computing had a 25% greater detection rate.

According to Cardoso *et al.* [11], complex event processing (CEP) technology, which permits real-time analysis and processing of data to identify DDoS assaults in edge computing to achieve quick reaction time, has been suggested. The suggested system is divided into three phases, each of which is described: Stages of data analysis and stage of assault detection. Finally, there is the preventative stage, where the proposed system CEP achieved excellent accuracy in detecting DDoS assaults in real time, but the fraction of missing data exceeds 8%, which is irrational given the high accuracy acquired.

Shrivastava *et al.* [12] developed a support vector machine (SVM) model to gather assaults on IoT devices while employing the cowrie honeypot as a collection tool. They classified the attacks into different types using machine learning algorithms (namely, naive bayes, jrandom forest, j48 decision tree, and SVM) and evaluated its performance using machine learning algorithms (namely, random forest, naive bayes, J48 decision tree, and SVM) with accuracy ranging from 67.7% to 97.39%.

A methodology for detecting DDoS assaults in fog computing is proposed by Cardoso *et al.* [13] utilizing a Raspberry Pi 3B as a fog server. Denial of service (DoS) and DDoS assaults are generated with the help of the HPING3 application (SYN Flood, Ping Flood, and UDP Flood). They conducted a simulation to determine the resources required to prevent DoS and DDoS assaults, and the findings revealed that the capacity to identify and block the addresses of attackers took less than 20% of the CPU and 1% of the RAM, respectively.

Maharaja *et al.* [14] presented a fog computing-based security system (FOCUS) to identify DDoS threats. To protect the connection to IoT devices in their system, they primarily used a virtual private network (VPN), followed by an authentication approach to identify malicious assaults. Using tree classification and challenge-response authentication, a mixed fog environment was used to create the system, with 80% of requests being handled in the fog environment and 20% in the cloud environment, where the system can effectively filter threats. The FOCUS approach was shown to be the most effective in terms of attaining minimal latency and resource consumption.

Almiani *et al.* [15] suggested a completely automated method for intrusion detection that was based on artificial intelligence. Because it is so near to IoT devices, the suggested model makes use of multi-layer recurrent neural networks that are specifically developed to offer the necessary safety for fog computing. The backpropagation method is used for classification in order to distinguish between normal and abnormal situations. The accuracy of the system's performance was determined using the NSL-KDD dataset, which had a precision of 94.27%. The model demonstrated significant susceptibility to DoS assaults.

A fog computing approach was used by Zhou *et al.* [16] to mitigate DDOS attacks in three stages: the first stage involved a firewall capable of filtering botnet attacks in real time, the second stage involved using network functions to analyze traffic, and the third stage involved central coordination of connecting local servers to cloud services. The results showed that the detection rate of TCP protocol type attacks is 99.56% and Modbus is 70.35% in the fog level alone, while the detection rate of TCP protocol type attacks is 99.84% and Modbus is 88.02% in the fog computing approach.

Ahmed *et al.* [17] used two algorithms particle swarm optimization (PSO) and salp swarm algorithm (SSA) for scheduling work in a fog environment and proposed Markov chain models that consisted of two stages, the first to calculate average bandwidth in-network and the second to obtain an average number of virtual machines in network to detect DDoS attacks, in order to improve the accuracy of their results. In their evaluation, they discovered that the suggested technique may minimize the amount of tasks while also detecting threats. Making use of the iFogSim simulation software According to the researchers, the approach can ensure that fog computing functions properly while also minimizing DDoS assaults.

With the use of a cloudy computing environment and an intrusion detection system (IDS) intrusion detection system, Kumar *et al.* [18] proposed a distributed ensemble design based on an IDS that improved the collection and speed of data processing large amounts of data due to its proximity to IoT devices. The planned system was split into three stages, which were as follows:

This is the initial step, which involves pre-processing the data and identifying any missing information. After that, algorithms such as K-NN, XGBoost, and Gaussian naive bayes are used to gather data and determine the deviation from the mean in order to enhance the detection rate of assaults. Second-level predictive findings are used in the third step of the process to enable legitimate traffic while blocking fraudulent traffic. In tests conducted using the UNSW-NB15 and DS2OS datasets, the system was analyzed and found to be effective in detecting 68.98% of analysis, 92.25% of reconnaissance, 85.42% of DoS assaults, and 71.18% of backdoor attacks [18].

Using fog computing for quick and precise detection, the authors of Shaikh *et al.* [19] offer a framework for mitigating DDoS assaults on the IoT. A database that maintains signatures of previously identified assaults (CICDoS 2019) was utilized in conjunction with skew-based mitigation, which use the k-NN classification method to identify DDoS attacks. They said that the model would be able to identify DDoS assaults with a high degree of accuracy (99.99%).

Souza *et al.* [20] proposed a hybrid binary classification approach that proposes the use of deep neural networks (DNN) and the k-nearest neighbor (kNN) algorithm for IoT intrusion detection in the fog computing layer to detect threats faster and to reduce the amount of time it takes to detect threats. They divided the occurrences into two categories: those that were attacks and those that were not. Using publicly available datasets (NSL-KDD and CICIDS2017), they analyzed their work and discovered that the technique has a high accuracy in identifying assaults (99.77% NSL-KDD dataset and 99.85% CICIDS2017 dataset).

Research by Li *et al.* [21] are attempting to develop a framework for detecting DDoS assaults using federated learning in fog computing. FLEAM is a streamlined, scalable approach for reliably and easily detecting zombies. It is particularly useful when used in conjunction with the UNSW NB-15 dataset, and it has an accuracy of 98%. DDOS attacks were detected in two parts by Bishnoi *et al.* [22] using deep learning in a fog environment. The first part used long short-term memory (LSTM) to classify the attacks into two categories, benign and harmful; the second part used convolutional neural networks (CNN) to classify the data, with accuracy reaching 86% in both parts.

A fog-based framework for detecting DDoS assaults is proposed by Gaurav *et al.* [23]. Clustering and entropy are two methods of data analysis. The simulations used in this paper were created using the ommnet++ simulations. It is claimed that their method identifies DDoS assaults with a high degree of efficiency [23].

3. METHOD

The work technique is divided into two layers: the first is the IoT devices layer, and the second is the fog layer. As stated in Figure 2, below is detailed explanation of the proposed system:

3.1. IoT layer

3.1.1. Reading sensor data

In addition to the two Raspberry Pi 400 with 4GB RAM, reading sensor data is the act of gathering data from IoT devices that detect it from their environs, such as smart devices, security systems, health meters, and other devices mentioned in Table 1. It may be called a programmable computer that offers communication support for a variety of network protocols and peripherals owing to its small size and low cost. Because of its tiny size and low cost, the Raspberry Pi is a performance-efficient computer.

3.1.2. Pre-processing and encoding data

It is seen as a critical stage in the IoT since it involves collecting irregular data and transforming that data into regular data. To put it another way, it is the process of turning data into a more apparent shape and a comprehensible format so that can extract and process information from it. The data is then delivered to the fog layer for processing.

3.1.3. Fog layer

Fog computing is a decentralized system in which heterogeneous devices connect with one another for the purposes of computing, processing, and storing with the least possible disturbance. It is critical to conduct correct computations, assess data, and identify potentially dangerous situations [24].

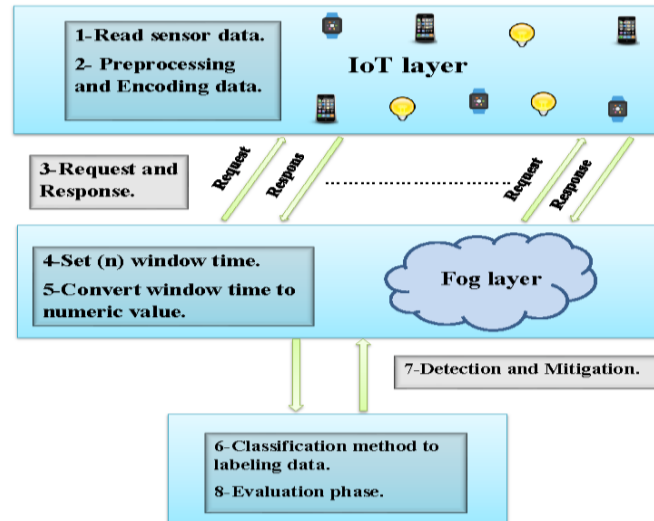


Figure 2. Flowchart of the proposed system

Table 1. Sensor type

Device	Model	Output type	Range	Voltage
Temperature sensor	DS18B20	Digital	-55 to +125 °C	3 to 5.5 V
Temperature sensor	DS18B20	Digital	-55 to +125 °C	2.7 to 5.5 V
Temperature and humidity sensor	DHT11	Digital	Temperature: 0°C to 50°C Humidity: 20% to 90%	3.5V to 5.5V

3.1.4. Set (n) window time

Shown in Figure 2 the fourth stage of the suggested system, since it is one of the primary processes in which data is fetched in real-time, and many programs (Wireshark, TCPtrace, QPA, Tstat, and Xplico), which are strong tools for studying traffic networks, support this need. Wireshark, which is one of the most significant network data analysis software packages, will be used in this investigation. It is free and open-source, and it may be installed on Windows computers. The data will be retrieved every two (2) seconds until it has been thoroughly examined. During the packet analysis process, Wireshark selects four attributes from the packet's (source address, destination address, source port, and destination port) to be evaluated and attacks identified.

3.1.5. Convert window time to numeric value

To detect DDOS assaults, it is necessary to measure the randomness of the network using the entropy. The notion of entropy was introduced for the first time by the scientist Claude Shannon in his article "A Mathematical Theory of Communication" published in the year 1948 [25]. This is known as the entropy principle. It is possible that the entropy is large, which suggests that the random distribution is high, but it is also possible that the entropy is zero, which implies that all values are the same. This idea may be used to identify DDOS assaults based on the parameters of the packet (source-destination-source-port-destination port) and the calculation of randomness. A collection of packets' entropy is calculated, with the number 1 indicating that the randomness is high and 0 indicating that the packets are all identical to one another. The general formula of entropy:

$$H(X) = -\sum_{i=1}^n p(x_i) \log_2(p(x_i)) \quad (1)$$

Where $H(X)$ is entropy of X , X is discrete random variable, $P(x_i)$ is possible outcomes (x_1 to x_n), which occur with probability $P(x_1)$ to $P(x_n)$

3.1.6. Classification methods

It is the process of determining which category the new information will go into. Using classification, both regular and irregular data may be grouped together. A classification system may be thought of as a method of studying and finding items to learn that are organized into categories. As the data is trained on the dataset CIC-DDoS2019 Benchmark, the proposed system uses k-nearest neighbors (KNN) algorithms to categorize the data, and the proposed system utilize the data to forecast what the next data will be in suggested model. To

do this, remove the properties from the dataset CIC-DDoS2019 Benchmark that don't need and keep only four properties (source IP, destination IP, source-port, destination-port) so that the KNN algorithm can calculate the dimension of the new point in real-time that has been transformed using entropy with the trained data to determine whether the point is close to attacking or normal.

Algorithm 3. Pseudo code of a KNN algorithm [26]

1. Start
2. Load the data.
3. Set the value of K to its initial value.
4. Taking into account each point in the testing set consists of:
Calculate the distance between the testing data and all rows of the training set using the (Euclidean distance) formula.
 - 4.1. Sort the distances that have been calculated in ascending order based on the distance value.
 - 4.2. Choose the first K rows from the sorted array.
 - 4.3. Find the class that appears the most often in these rows.
 - 4.4. Return the projected class label.
5. End.

3.1.7. Detection and mitigation

At this point, the malicious data that caused the DDoS attack is known. The propose system select the source IP and added it to block list in the Realtime environment as shown in Figure 3.

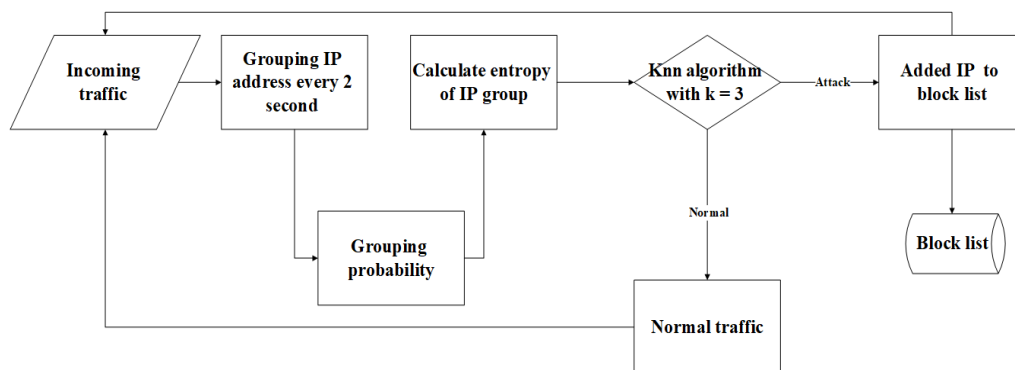


Figure 3. Block list IP address datagram of the proposed

4. RESULTS AND DISCUSSION

While the fog layer consists of a computer with characteristics like (Windows 10, core i7, 12 GB of RAM, 500GB SSD hard drive and system type 64bit), the IoT layer consists of two Raspberry Pi 400 devices each with 4 GB of RAM and a microSD card slot. Two sensors are included inside each Raspberry Pi 400 computer (waterproof sensor and temperature-humidity sensor) as shown in Figure 4. The sensors detect changes in the surrounding environment and relay information to the fog layer below the fog layer. The programming language that uses in proposed system is Python.



Figure 4. Raspberry Pi 400 with waterproof sensor and temperature-humidity sensor

In the propose system used the scapy package to mimic DDoS assaults, which can carry out three different sorts of attacks (TCP, UDP, and ICMP attacks). These assaults were executed in the first raspberry in addition to the transmission of sensor data, while the second raspberry transmits just sensor data in the first raspberry. In the fog layer, the proposed system used the CIC-DDoS2019 Benchmark dataset to train the KNN algorithm, which was then applied to the dataset. The following is the initial algorithm for assessing the data that will be collected:

Algorithm 1 DDOS detection and classification use KNN algorithm

```

While to the incoming packet every (n) second and select
  (sourceIP, destinationIP, source-port, destination-port) do
    Filter packet for null:
      | pass;
    end
    Calculate probability of group IP and port;
    Calculate entropy of group IP and port;
    IF the distance of the new point is close to the attack then
      | DDOS attack is detect and mark packet;
      | Added IP to group of block list;
    end
    Else
      | The traffic is normal and mark packet;
    End
  End
End

```

The proposed system utilized real-time data to put our suggested concept into action. Every two seconds, it gathers packets and extracts four attributes from each packet number of packets, at the maximum of every two seconds 67 packets are collected. For each set of addresses, it is evaluated the probability of each address and then calculate the randomness using entropy to arrive at a final result of four points.

Continuing to work, sends the four points to the KNN algorithm, CIC-DDoS2019 Benchmark dataset was used for training, and K=3 was determined by utilizing euclidean distance (2) to establish the value of K=3.

$$Dist = \sqrt{(x1 - y1)^2 + (x2 - y2)^2} \quad (2)$$

Using the four points as input, the algorithm calculates the distance between them and the sum of the trained points. In cases where the points are near to the sum of the attack points, the packets are tagged with the attack type (1); in cases where the points are close to normal points, the packets are marked with the normal type (0). The suggested system operated for 600 seconds while being subjected to DDoS assaults during certain intervals of time during which conducted three kinds of real-time attacks on it (TCP, UDP, and ICMP attacks). With excellent results, the suggested system obtained 100% detection accuracy for TCP attacks, 98.79% detection accuracy for UDP attacks, and 100% detection performance accuracy for ICMP attacks. Accuracy is a statistical measure used to evaluate the classification algorithm performance as shown in (3)

$$ACC = \left(\frac{TP+TN}{TP+TN+FP+FN} \right) \quad (3)$$

Where ACC is accuracy, TP is true positive, TN is true negative, FP is false positive, FN is false negative.

$$TruePositive\ rate = TP / (TP + FN) \quad (4)$$

$$True\ Negative\ rate = TN / (TN + FP) \quad (5)$$

$$False\ Positives\ rate = FP / (FP + TN) \quad (6)$$

$$False\ Negatives\ rate = FN / (FN + TP) \quad (7)$$

The results are shown in Table 2. Using the sliding window, figuring out the entropy for the sliding window, and entering it into the KNN algorithm gives the possibility of high-accuracy detection for the proposed system. Figure 5 shows that proposed system is able to detect DDoS attacks, sort normal packets from abnormal ones, and blacklist the abnormal ones.

Table 2. TCP, UDP and ICMP attacks accuracy rate

	TP	TN	FP	FN	F1-SCORE	PRECISION	RECALL	ACCURACY
TCP	1.0	1.0	0.0	0.0	1.0	1.0	1.0	1.0
UDP	1.0	0.96	0.04	0.0	0.99	0.99	0.99	0.9879
ICMP	1.0	1.0	0.0	0.0	1.0	1.0	1.0	1.0

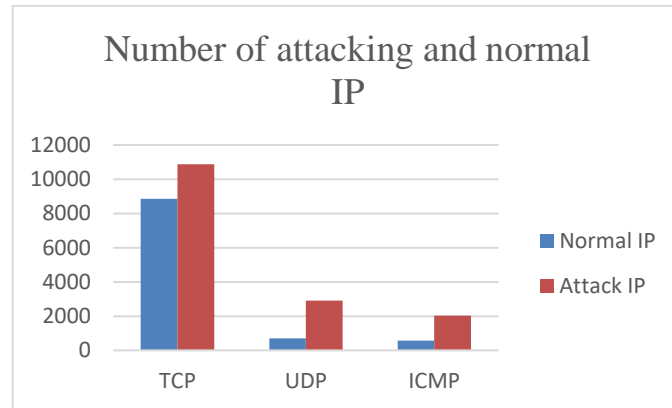


Figure 5. Number of attacking and normal IP

Table 3 compares the proposed system to related works in terms of real-time use, advantage, and disadvantage. The proposed system, when compared with its peers, shows that it is able to detect DDoS attacks with high accuracy and speed. Table 4 shows that our proposed system is better at detecting three types of DDoS attacks with high accuracy and with little to no false positives when some attacks are found.

Table 3. Result comparison

Author	Real time	Method	Advantage	Disadvantage
[10]	No	OS-ELM	High accuracy rate	Using legacy dataset (public databases NSL-KDD)
[11]	Yes	CEP	Good accuracy rate	percentage of missing data reaches 8%
[12]	No	SVM and etc.	Multiclass detection	Low accuracy rate and time
[13]	Yes	-	Reduce resource use	Not mentioning the methods used for detection
[14]	Yes	FOCUS	Efficient	VPNs might slow down your internet connection.
[15]	No	DRNN	Low time for detection	Low accuracy rate
[16]	Yes	NFV DDoS analysis	High accuracy rate	Only TCP flood attack detected
[17]	No	Markov chain models	Minimizing the number of offloaded tasks	Low accuracy rate
[19]	No	KNN	Good accuracy rate	Not implemented in real time
Our approach	Yes	Entropy and KNN	High accuracy rate and low time for detection DDoS attack	-

Table 4. Compare results

Author		TCP flood	UDP flood	ICMP flood
[11]	True positives	94.09%	98.75%	95.43%
	False positive	6.96%	0.75%	1.25%
	Accuracy	93.10%	99.24%	98.70%
[16]	True positives	-	-	-
	False positive	-	-	-
	Accuracy	99.56%	-	-
Our approach	True positives	100%	100%	100%
	False positive	0.0%	0.04%	0.0%
	Accuracy	100%	98.79%	100%

5. CONCLUSION

In this research, work was done on the fog layer's architecture using a real-time machine learning technique to identify DDoS threats. The fog layer is seen as an intermediate between IoT devices and the cloud layer; owing to its closeness to IoT devices, it is capable of detecting assaults early. Analyzing all incoming packets, extracting four parameters from each packet (source IP, destination IP, source-port, destination-port),





Detection and mitigation of DDoS attacks in internet of things using ... (Karrar Falih Hassan)

calculating the likelihood, then calculating the entropy, then submitting the data to the k-nearest neighbour method to assess whether or not there is an attack. The proposed system achieved 100% detection accuracy for TCP attacks, 98.79% detection accuracy for UDP attacks, and 100% detection accuracy for ICMP assaults. Our suggested system was able to identify and handle assaults early to decrease hardware effort. In the future, we intend to identify new kinds of DDoS assaults and reach high rates of detection in real-time with more data about DDoS attacks on various levels of the fog computing environment.





REFERENCES

- [1] R. Mahmoud, T. Yousuf, F. Aloul and I. Zuolkernan, "Internet of Thing (IoT) security: Current status, challenges and prospective measures," *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015, pp. 336-341, doi: 10.1109/ICITST.2015.7412116.
- [2] S. Li, L. Da Xu, and S. Zhao, "5G IoT: A survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1-9, 2018, doi: 10.1016/j.jii.2018.01.005.
- [3] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the IoT," *MCC'12 - Proc. 1st ACM Mob. Cloud Computing Work*, pp. 13-15, 2012, doi: 10.1145/2342509.2342513.
- [4] A. Rauf, R. A. Shaikh and A. Shah, "Security and privacy for IoT and fog computing paradigm," *15th Learning and Technology Conference (L&T)*, 2018, pp. 96-101, doi: 10.1109/LT.2018.8368491.
- [5] D. H. Hoang and H. D. Nguyen, "A PCA-based method for IoT network traffic anomaly detection," *20th International Conference on Advanced Communication Technology (ICACT)*, 2018, pp. 381-386, doi: 10.23919/ICACT.2018.8323766.
- [6] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," *IEEE 23rd International Multi-topic Conference (INMIC)*, 2020, pp. 1-6, doi: 10.1109/INMIC50486.2020.9318216.
- [7] R. R. Brooks, I. Ozcelik, L. Yu, J. Oakley and N. Tusing, "Distributed Denial of Service (DDoS): A History," *IEEE Annals of the History of Computing*, 2021, doi: 10.1109/MAHC.2021.3072582.
- [8] M. Dimolianis, A. Pavlidis and V. Maglaris, "SYN Flood Attack Detection and Mitigation using Machine Learning Traffic Classification and Programmable Data Plane Filtering," *24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2021, pp. 126-133, doi: 10.1109/ICIN51074.2021.9385540.
- [9] M. De Donno, N. Dragoni, A. Giarretta and A. Spognardi, "Analysis of DDoS-capable IoT malwares," *Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2017, pp. 807-816, doi: 10.15439/2017F288.
- [10] S. Prabavathy, K. Sundarakantham and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in IoT," *Journal of Communications and Networks*, vol. 20, no. 3, pp. 291-298, 2018, doi: 10.1109/JCN.2018.000041.
- [11] A. M. da S. Cardoso, R. F. s Lopes, A. S. Teles, and F. B. V. Magalhães, "Poster Abstract: Real-Time DDoS Detection Based on Complex Event Processing for IoT," *IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018, pp. 273-274, doi: 10.1109/IoTDI.2018.00036.
- [12] R. K. Shrivastava, B. Bashir, and C. Hota, "Attack detection and forensics using honeypot in IoT environment," *International Conference on Distributed Computing and Internet Technology*, vol. 11319, no. 402-409, 2019, 2019.
- [13] J. V. Cardoso, H. V. Sampaio, C. A. Souza, and C. B. Westphall, "DoS attack detection and prevention in fog-based intelligent environments," *Brazilian Journal of Development*, vol. 5, no. 11, pp. 23934-23956, 2019, doi: 10.34117/bjdv5n11-089.
- [14] R. Maharaja, P. Iyer, and Z. Ye, "A hybrid fog-cloud approach for securing the IoT," *Cluster Computing*, vol. 23, no. 2, pp. 451-459, 2020, doi: 10.1007/s10586-019-02935-z.
- [15] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep Recurrent Neural Network For IoT Intrusion Detection System," *Simulation Modelling Practice and Theory*, vol. 101, 2020, doi: 10.1016/j.simpat.2019.102031.
- [16] L. Zhou, H. Guo, and G. Deng, "A fog computing based approach to DDoS mitigation in IIoT systems," *Computers & Security*, vol. 85, pp. 51-62, 2019, doi: 10.1016/j.cose.2019.04.017.
- [17] O. H. Ahmed, J. Lu, A. M. Ahmed, A. M. Rahmani, M. Hosseinzadeh, and M. Masdari, "Scheduling of Scientific Workflows in Multi-Fog Environments Using Markov Models and a Hybrid Salp Swarm Algorithm," *IEEE Access*, vol. 8, pp. 189404-189422, 2020, doi: 10.1109/ACCESS.2020.3031472.
- [18] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed ensemble design based intrusion detection system using fog computing to protect the IoT networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9555-9572, 2021, doi: 10.1007/s12652-020-02696-3.
- [19] R. A. Shaikh, S. R. Hassan, and M. A. Lawal, "A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing," *Procedia Computer Science*, vol. 182, pp. 13-20, 2020, [Online]. Available: <https://doi.org/10.1016/j.procs.2021.02.003>.
- [20] C. A. de Souza, C. B. Westphall, R. B. Machado, J. B. M. Sobral, and G. dos S. Vieira, "Hybrid approach to intrusion detection in fog-based IoT environments," *Computer Networks*, vol. 180, 2020, doi: 10.1016/j.comnet.2020.107417.
- [21] J. Li, L. Lyu, X. Liu, X. Zhang and X. Lyu, "FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4059-4068, 2022, doi: 10.1109/TII.2021.3088938.
- [22] S. Bishnoi, S. Mohanty and B. Sahoo, "A Deep Learning-Based Methodology in Fog Environment for DDOS Attack Detection," *5th International Conference on Computing Methodologies and Communication (ICCMC)*, 2021, pp. 201-206, doi: 10.1109/ICCMC51019.2021.9418363.
- [23] A. Gaurav, B. B. Gupta, C. -H. Hsu, S. Yamaguchi and K. T. Chui, "Fog Layer-based DDoS attack Detection Approach for Internet-of-Things (IoTs) devices," *IEEE International Conference on Consumer Electronics (ICCE)*, 2021, pp. 1-5, doi: 10.1109/ICCE50685.2021.9427648.
- [24] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," *Proceedings of the 2015 Workshop on Mobile Big Data*, 2015, vol. 2015, pp. 37-42, 2015, doi: 10.1145/2757384.2757397.
- [25] G.F.S., "The Bell system technical journal," *The Bell system technical journal*, vol. 196, no. 4, pp. 519-520, 1923, doi: 10.1016/s0016-0032(23)90506-5.
- [26] S. Mishra, P. K. Mallick, H. K. Tripathy, L. Jena, and G. S. Chae, "Stacked KNN with hard voting predictive approach to assist hiring process in IT organizations," *The International Journal of Electrical Engineering & Education*, 2021, doi: 10.1177/0020720921989015.

BIOGRAPHIES OF AUTHORS

Karrar Falih Hassan     Obtained the BS degree in Information Networks, College of Information Technology, University of Babylon, Iraq in 2013-2014. He is currently pursuing the M.E. degree in the Information Networks Department, College of Information Technology, Babylon University, Iraq. Research interests include the IoT, wireless network security and machine learning. He can be contacted at email: karrar.alhashimi22@gmail.com.



Mehdi Ebady Manaa     is currently an assistant professor in the department of information network, College of Information Technology, University of Babylon. He received his bachelor's degree from the University of Babylon, college of science in 1999-2000. His master of science from University Utara Malaysia (UUM), Malaysia in 2012. He received his PhD in Computer Science and in the field Network Security and Data Mining using Cloud Computing from the University of Babylon, College of Information Technology in 2016. He is currently focusing on the detection of the attacks. The main interesting fields are data mining techniques (clustering and classification), communication software, network security, cloud computing, IoT, and unstructured data. He can be contacted at email: it.mehdi.ebady@itnet.uobabylon.edu.iq.