An efficient IDS using FIS to detect DDoS in IoT networks

Trong – Minh Hoang1,Nhat – Hoang Tran1, Vu – Long Thai1,Anh – Thu Pham1

1 Posts and Telecommunications Institute of Technology Hanoi City, Vietnam

[hoangtrongminh@ptit.edu.vn](mailto:hoangtrongminh@ptit.edu.vn), [hoangtn.B18VT178@stu.ptit.edu.vn](mailto:hoangtn.B18VT178@stu.ptit.edu.vn), [longtv.B18VT268@stu.ptit.edu.vn](mailto:longtv.B18VT268@stu.ptit.edu.vn), thupa@ptit.edu.vn

*Abstract*— The growing IoT applications of today have brought numerous benefits to our lives. In addition, cyber-attacks are growing as a result of increasingly sophisticated and violent attacks. Detection systems that serve as security protection against emerging attacks are also being developed using machine learning techniques. However, many additional challenges continue to emerge as demand for IDS deployment at the edge network, where resource-constrained devices exist, continues to increase. These devices require a database with a high level of accuracy for attack detection. This research provides a Fuzzy-based IDS for detecting DDOS attacks with a 99 percent accuracy rate that is deployable on edge computing using the IoT23 dataset.

Keywords— Internet of Things (IoT), IDS, Fuzzy Inference System, DDOS, IoT 23 dataset.

# Introduction

With the advancing growth in technology in the current digital age, the Internet of things (IoT) has become crucial in our daily lives. The IoT has a massive collection of intelligent devices connected to a network to send and receive large amounts of data to and from other devices. The IoT could allow access, control and manage these devices to provide various functionalities in many applications such as smart homes, smart healthcare, smart transportation, smart industry... [1] [2]. Therefore, an enormous amount of data is sent to the cloud by IoT devices for further processing and analysis. As a result, centralized cloud processing is unsuitable for numerous IoT applications due to high delay, network failure, or packet loss. At that time, the rise of edge computing with the IoT systems addressed these issues by providing the computational capacity near the data-generating devices. In other words, the IoT system with edge computing allows IoT data to be gathered and processed at the edge, rather than sending the data back to a data center or cloud.

Besides the advances in edge computing, edge devices are susceptible to many kinds of attacks, such as Denial of Service (DoS), Distributed Denial of Service (DDoS), and man-in-the-middle attacks [3-5]. In which the Distributed Denial of Service (DDoS) attack is one of the leading security challenges in IoT networks; it degrades resources to make them unavailable for legitimate users. The DDoS attacks have different forms, and each has its behavior of overwhelming or wasting resources to achieve its goal [6].

Many security solutions like firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) are now applied to protect the devices from cyberattacks. IDS is the most competent mechanism for detecting DDoS in the first barrier. It is a system that monitors the network for suspicious events and generates a report to the administrator to take action against it. Nevertheless, the traditional approaches of IDS systems have crisp boundary problems [7-10] and cannot defend against the complex DDoS attacks [11-13]. Hence, intrusion detection techniques should be improved to keep up with the complexity of DDoS threats. Researchers have recently paid attention to the IDS solutions based on artificial intelligence (AI) detection methods such as machine learning and deep learning because of their advantages in network anomaly detection. However, these approaches require large quantities of data to build the detection models and are pretty complicated. Moreover, several IDSs using fuzzy logic, which offers several advantages to handling crisp boundary problems [14], have been suggested as one of the most efficient solutions to defend against DDoS attacks. In the IDS system, fuzzy rules can be employed to identify the normal and abnormal behavior, and fuzzy inference logic can be applied to such rules to determine when an intrusion is in progress.

In practical cases, the datasets are essential to evaluate the feasibility of any proposed IDS system. Up to now, many different datasets have been applied in the studied anomaly detection frameworks. Some popular datasets are DARPA, KDD-Cup'99, NSL-KDD, CICDDoS 2019, ISOT, CTU, and UNSW-NB [15,16]. These datasets may cause an outage and are not suitable for IoT networks. In 2020, the IoT-23 dataset with 20 malicious captures executed in IoT devices and 3 captures for benign IoT device traffic was published to explore generative deep learning techniques that can automatically detect and classify IoT cyberattacks. Hence, To handle the detection of modern attack patterns, we use the IoT23 dataset in testing our proposed method.

This paper proposes a novel IDS system based on a fuzzy inference system (FIS) to detect DDOS attacks on little IoT 23 with high accuracy so that edge computing can be deployed. The proposed model enables a favorite attack detection approach with high accuracy, low false-positive rates, and scalability compared to existing methods.

The rest of this paper is organized as follows. After considering the related works in section II, the proposed system is presented in section III. Numerical results and discussion are presented in Section IV. The last section concludes the paper and offers ideas for future work.

# Related work

IDS has emerged as one of the most common parts of network security infrastructure. IDS is usually classified into signature-based IDS and anomaly-based IDS. In signature-based IDS, detection techniques usually utilize the previously known attack patterns to detect attacks. On the other hand, anomaly-based IDS focuses on detecting unusual activity patterns in the observed data. In other words, they can detect novel attacks without prior knowledge. Up to now, malicious attacks have become more sophisticated and obfuscated to identify. Consequently, developing an efficient IDS to detect DDoS attacks is necessary for complex environments such as IoT networks.

The authors in [17] proposed an IDS in which fuzzy logic is employed to decrease uncertainty in abnormal decisions. They analyzed their model on the CICDDoS dataset to evaluate their proposed model. They proved that the scheme could improve the detection rate of DDoS attacks more than other methods. In [18], the authors used a fuzzy-based abnormal detection method using the KDD-Cup'99 dataset to validate the solution. This approach shows that the false-positive rate is low and the detection rate is high. Another fuzzy detection scheme is presented in [19]. That is a secure MQTT approach to recognize abnormal traffic in IoT devices and protect them against DDoS attacks. In [14], anomaly-based IDS uses a fuzzy inference system to detect DDoS attacks. The suggested framework was applied to the DDoS 2016 dataset. The results show that the true-positive rate is 91.1%, and the false-positive rate is 0.006%. Various other studies are focusing on the schemes in which FIS is used to build abnormal detection systems in different environments like SDN [20] [21], WSN [22], and cloud computing [23].

However, only a few fuzzy-based IDS is designed for currently distributed IoT environments. Some reliable and effective fuzzy-based IDS proposals for IoT networks against DDoS attacks have been published [1] [2] [18] [19] [24]. Nevertheless, these proposals are only based on outdated datasets which may not include the modern reflective DDoS attacks, and there is almost no comparison between different datasets. Furthermore, some datasets are not captured from the IoT device network. In [25], the IDS is based on the FIS model for detecting abnormal issues. In a statistics-based algorithm, every new traffic network measure is compared to the referenced free traffic distribution to detect the DOS and DDOS attacks. It can bring better accuracy of detection methods based on previously statical methods. However, the proposed model is essential to theoretical while does not apply to a practical dataset.

Developing solutions to detect DDOS at the edge of the network brings great benefits to network operators by reducing most of the data traffic that must be transmitted to the computing center. The authors in [26] demonstrate that their smart defense solution can migrate 90% of DDOS traffic using IDS at the edge. The author in [27] uses a statistical method with a variant of the CRPS algorithm to propose the anomaly detection framework to prevent DDoS attacks in fog-empowered IoT networks. The proposed protocol used the DARPA99 database to adapt to fog devices, which reduced dimension by the principal component analysis (PCA) method. Although the proposed protocol can detect the TCP-SYN and ICMP attacks, it is not evaluated by specific performance parameters such as accuracy or true/false alarm metrics. Thus, the classification and dimensionality reduction for the data set is a core condition for deploying IDS at network edge devices with limited resources [26] [27] [28].

The datasets utilized for attack detection are crucial, as they represent actual attack patterns and have distinct data properties that directly impact the IDS system's performance. In the last few years, researchers have focused their attention on the frameworks for IDS in IoT networks evaluated by the IoT23 dataset [29-33], a new dataset of malicious and benign networks created by the Avast AIC laboratory in 2020. The results of the studies revealed that the suggested models were appropriate for developing an efficient anomaly-based intrusion detection system for IoT networks with high accuracy, precision, recall, and F1 score. Besides, machine learning or deep learning algorithms are explored in these approaches to build the detection models in IoT networks. As a result, these frameworks are complex and therefore unsuitable for IoT with edge computing.

Moreover, the IoT23 dataset is a large dataset with many features. Hence, we utilized the IoT little database for our proposal. In more detail, A fuzzy intrusion detection system using a little IoT23 dataset is employed FIS with PSO algorithm to optimize fuzzy rules, bring a high accuracy rate, and is desirable for IoT networks employing edge computing. To the best of our knowledge, this type of framework has not been explored in the literature.

# Proposed system

## Background

**Fuzzy Inference System**. Fuzzy Logic Theory is a kind of soft computing approach to deal with real-world problems that are hard to consider as completely "true or false" (the binary decision problems) and can solve these problems with solutions that are close to natural human decisions. A Fuzzy Inference System (FIS) is a system that uses a fuzzy set theory to map input variables to an output space. The basic model of a FIS system is described in figure 1.

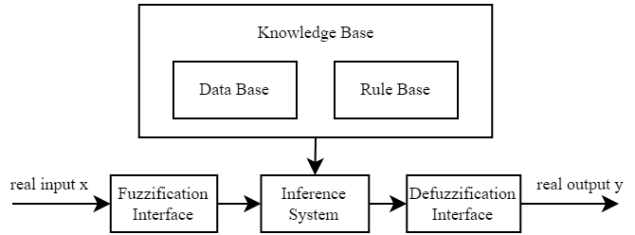


Fig. 1. The basic model of a FIS system

In the fuzzification step, input values are converted into degrees of membership with the help of membership functions. The "IF-Then" rules describe the relationship between inputs and outputs. The fuzzy inference applies the fuzzy "If-Then" rules to calculate the fuzzy output value from input values. Finally, in the defuzzification phase, the output values obtained from the inference are mapped to the specified value using appropriate methods. There are two well-known fuzzy inference methods: the Mamdani model and the Tsukamoto Sugeno model. In this study, the Mamdani system is utilized because of its more intuitive and easier-to-understand rule bases.

**Particle Swarm Optimization (PSO).** PSO is a meta-heuristic population-based optimization algorithm under the category of evolutionary algorithm. The particles move iteratively around the search space to find the global best location (the best solution). A fitness value is calculated to evaluate how good a particle's current location is. A record of the best location of each particle based on the fitness value is saved. In each iteration, a particle updates its velocity according to three components: its current velocity, its personal best previously visited location (pbest), and the location with the highest fitness value visited by any particle in the population so far (gbest). After several iterations, the best solution is obtained. The formulas for updating the velocity and location of a particle are:

 (1)

 (2)

Where *x(t)* and *v(t)* indicate the location and velocity of a particle at time *t*, respectively; *w* is the initial weight factor; *c1*and *c2*arelearning factors; *r1*and *r2*are uniformly distributed numbers in the range (0,1).

## Data processing

Data processing is the process of extracting network features from raw network traffic for training and evaluating models. These features are extracted from the *conn.log.labeled* file in the little IoT-23 dataset and exported to the file in CSV format. Because the model is designed for IoT networks, local network features such as stream ID, source IP address, destination IP address, and timestamp will be removed from the dataset. The index features of the dataset are coded and presented as binary data. The NaN values are substituted for 0. The featured columns are then normalized to a specified range [-1 1] to eliminate large values and speed up computation. Besides, we use feature selection to improve accuracy and reduce noise for the model. The appropriate features are selected through the recursive feature elimination technique. For missing data values in a feature column, we deal with them by replacing them with the average value of each corresponding attack type in that feature. The principal components analysis (PCA) technique is applied to the data to help reduce complexity, overcome resource constraints, and increase the performance of anomaly detection models.

After being processed and reduced in dimension, we select the dataset's secure (Benign) and DDoS patterns. This dataset is divided into 3 sets: Training\_set, Validating\_set, and Testing\_set. The number of samples in the Training\_set and the Testing\_set are taken equally. The number of samples in the Training\_set and Validating\_set are in an 80/20 ratio. The training\_set is a standard space for the following stages' calculations. Figure 2 shows the data processing system.

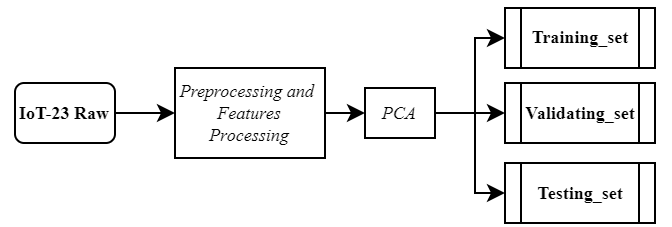


Fig. 2. Data processing system

## The proposed system

The proposed IDS uses the PSO algorithm to optimize the parameters for the FIS with a radius of *r*. The proposed system is simple and effective. Figure 3 shows the detail of the proposed system.

The FIS in which the Mamdani model is implemented has 2 inputs, including N\_benign, N\_ddos, and 1 output. Each input has 2 membership functions, L (Low) and H (High). The output has 3 membership functions that are FA (False Attack), MA (Medium Attack), and HA (High Attack) functions. Inference rules and output membership functions are fixed. Table I presents the rules of the FIS, and figure 4 shows the membership functions for the output of the FIS. The PSO algorithm optimizes the parameters of input membership functions and the radius r.

1. Rules of Fuzzy inference System

|  |  |  |
| --- | --- | --- |
| **N\_Benign** | **N\_DDoS** | **Output** |
| L | L | FA |
| L | H | HA |
| H | L | FA |
| H | H | MA |

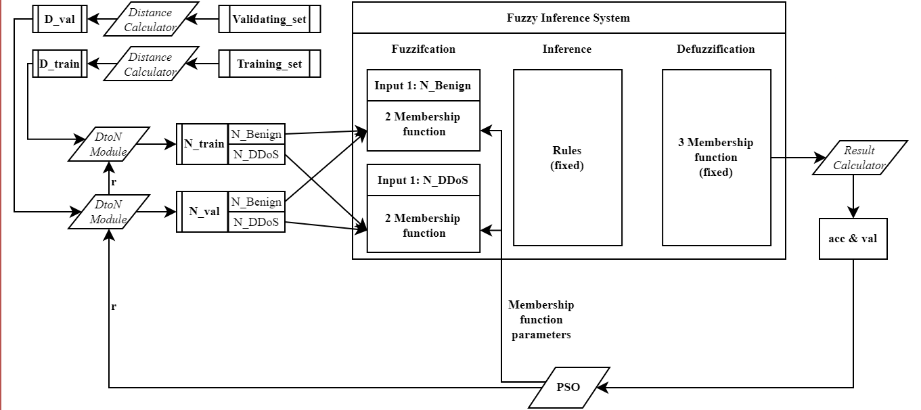


Fig.3. The proposed intrusion detection system

**

Fig. 4. Defuzzification Membership functions

Each input membership function has a trapezoid shape characterized by four parameters (*a, b, c, d*) and coded by three parameters (*x, y, z*) so that it is suitable for the PSO algorithm. The relationship of these parameters could be expressed as follows

 (3)

 (4)

 (5)

 (6)

Figure 5 describes the encodings of the membership function parameters. After being encoded, the parameters of the four membership functions of two inputs will be joined together and connected with radius r to form a particle for the PSO algorithm of length 13.

Two datasets, including Training\_set and Valid\_set, are fed into the system. In the Training\_set, the distance is calculated to the rest of the set points to obtain the D\_train distance matrix, D\_train. Moreover, the distance between each point in the Valid\_set and each point in Training\_set is calculated to obtain the distance matrix, D\_val.

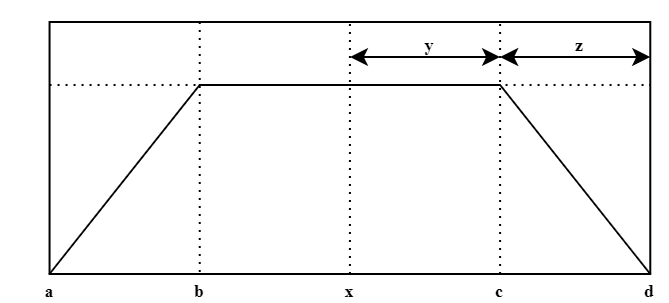


Fig. 5. The input membership function

The PSO algorithm randomly initializes n particles of length 13, with *r* in the range [0 avg(D\_train)] and the remaining parameters in the range [0 1]. In each round of the PSO algorithm, every particle receives parameters such as *r* and membership functions of inputs, then executes as:

Two distance matrices, D\_train and D\_val, and the radius r are two inputs of DtoN module. With a subset, the point is to find the neighbor points under the r ratio. Based on the labels of the points, the number of safe points (N\_benign) and the number of DDoS attack points (N\_ddos) in the two sets (Training\_set and Validating\_set) could be found. It is to build two matrices of N\_train and N\_val (there are 2 columns corresponding to N\_benign and N\_ddos), respectively. The two matrices are then divided by the maximum value in the N\_train matrix and limited to the interval [0 1].

The parameters of the two input membership functions are decoded into specific parameters and then fed into the FIS. Two matrices, N\_train and N\_val, are fed into the FIS to get the corresponding output. The output of the FIS is a value in the range [0 1]. The Result Calculator converts this output into 0 (Benign) or 1 (DDoS). The threshold value in the Result Calculator is 0.5. If the output value is more significant than 0.5, 1 (DDoS) have resulted. Otherwise, 0 (Benign) is decided. The results are then compared with the original labels of the Training\_set and Validating\_set to obtain *acc* and *val*, respectively. The PSO algorithm uses these two results to find the most optimal particle.

# 

Fig. 6. The experimental system

# Exprimental and results

## Experimental parameters and evaluations

All experiments of IDS using FIS are conducted using Matlab. Training\_set and Validating\_set are applied to optimize the FIS through the PSO optimization algorithm. The parameters of the PSO algorithm used in our simulation are shown in Table II.

1. PARAMETERS FOR PSO ALGORITHM

|  |  |
| --- | --- |
| **Parameter** | **Value** |
| population | 50 |
| constriction factor | c1 = 2  c2 = 2 |
| inertia factor | 1 |
| inertia factor reduction rate | 0.99 |
| Number of rounds | 50 |

The system is optimized and is evaluated by the set of Testing\_set. Fig. 7 presents how to evaluate the system. The system is evaluated through the parameters including accuracy, precision, recall, F1-score, and FPR (False Positive Rate).

The accuracy is calculated as the fraction of correct predictions over the total number of predictions. The parameter is formulated as follows:

(7)

The fraction of correctly identified positives defines the precision. It is written as

 (8)

The recall is the fraction of actual positives that were correctly identified. The parameter could be expressed as

 (9)

The F1-score can be interpreted as a harmonic mean of the Precision and Recall. Its formula is

 (10)

Finally, FPR is a measure of accuracy for a test. It is calculated as the ratio between the number of negative events wrongly categorized as positive (false positives) and the total number of actual negative events (regardless of classification).

 (11)

## Convergence evaluation

Figure 8 below shows the convergence process of the PSO algorithm to determine the optimal parameters for the two boundaries *acc* and *val*. After about 15 iterations, we find that the optimal points have been determined and stabilized. This shows that PSO has good support for finding optimal values for input membership functions.

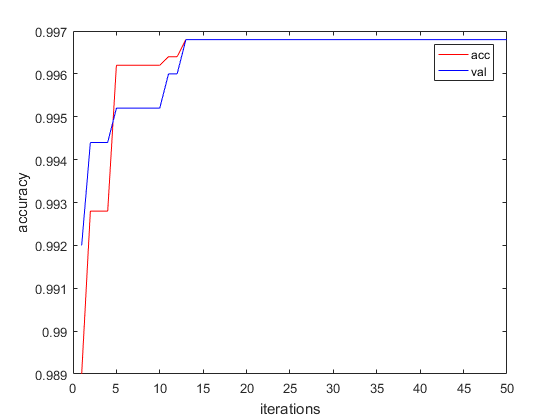


Fig. 8. The convergence rate of PSO

## Experimental results

With the parameters shown in table 2, the experimental system is run and evaluated on a Training\_set of 5000 samples which are reduced to have only 10 features. The optimal radius value is 1.0509, and the input membership functions of the FIS after optimization are presented in figure 9 and figure 10. The model after optimization is evaluated on testing\_set with 5000 samples which are entirely different from the samples in training\_set and validating\_set. The results are shown in Table III.

1. Experimental results on Testing\_set

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Accuracy** | **Precision** | **Recall** | **FPR** | **F1** |
| 0.998 | 1 | 0.995 | 0 | 0.998 |



Fig. 9. N\_Benign's Membership function

The experimental system also is implemented using different datasets which have a different number of samples and features. All experimental results give an accuracy of more than 99%. The results are detailed in Table IV and figure 10.



Fig. 10. N\_DDoS's Membership function

1. The experimental results on different datasets

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Samples** | **Features** | **Acc** | **Pre** | **Recall** | **FPR** | **F1** |
| **5000** | 32 | 0.999 | 0.998 | 0.999 | 0.001 | 0.999 |
| 23 | 0.997 | 0.997 | 0.996 | 0.003 | 0.997 |
| 16 | 0.998 | 0.996 | 1 | 0.004 | 0.998 |
| 10 | 0.998 | 1 | 0.995 | 0 | 0.998 |
| **2500** | 32 | 0.995 | 1 | 0.990 | 0 | 0.995 |
| 23 | 0.996 | 1 | 0.993 | 0 | 0.996 |
| 16 | 0.996 | 1 | 0.993 | 0 | 0.996 |
| 10 | 0.996 | 1 | 0.992 | 0 | 0.996 |
| **1000** | 32 | 0.994 | 0.996 | 0.992 | 0.004 | 0.994 |
| 23 | 0.996 | 1 | 0.992 | 0 | 0.996 |
| 16 | 0.995 | 1 | 0.990 | 0 | 0.995 |
| 10 | 0.994 | 1 | 0.988 | 0 | 0.994 |
| **500** | 32 | 0.990 | 1 | 0.980 | 0 | 0.990 |
| 23 | 0.990 | 1 | 0.980 | 0 | 0.990 |
| 16 | 0.990 | 1 | 0.980 | 0 | 0.990 |
| 10 | 0.994 | 1 | 0.988 | 0 | 0.994 |

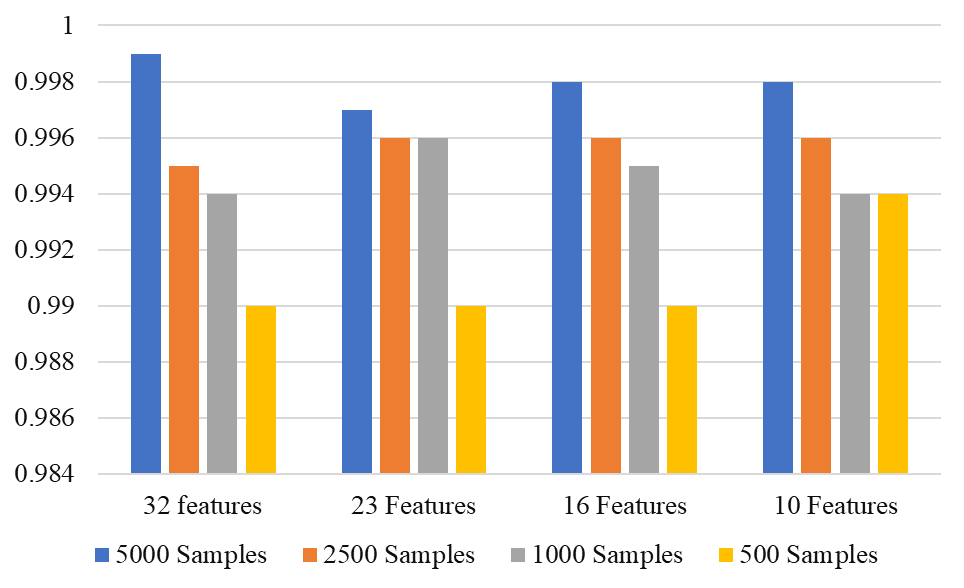
**

Figure 11: The experimental results in a bar chart

The test results show that our proposed system's DDoS attack detection and detection capabilities are better than that of the IDS system in [34] on the same IoT23 dataset. The maximum accuracy in [34] is 84.8%, while the maximum accuracy from our system is 99.9%. In addition, we tested with different numbers of samples and gave an accuracy of over 99%.

# Conclusion

In addition to the great benefits of IoT and edge computing for the infrastructure and applications of communications networks, new IDS-related difficulties emerge. Developing an effective IDS with the limited resources of IoT devices is a challenge to overcome. This paper presents an IDS model for detecting DDOS attacks that can be deployed on edge devices. Using PSO-optimized FIS, our proposed model produced amazing results compared to previously proposed methods. The detection accuracy of DDOS attacks is up to 99.9%, with IoT23 database sample sizes fully deployable on edge devices. Even with the minor test samples, 99 percent accuracy was achieved. In our future works, we will deploy the proposed model on practical IoT devices.

##### References

1. [Faisal Hussain](https://ieeexplore.ieee.org/author/37088388829), [Syed Ghazanfar Abbas](https://ieeexplore.ieee.org/author/37088641728), etc. "IoT DoS and DDoS Attack Detection using ResNet" [2020 IEEE 23rd International Multitopic Conference (INMIC)](https://ieeexplore.ieee.org/xpl/conhome/9318042/proceeding), pp. 1-6, 2020.
2. Mohammed Hasan Ali, etc. "Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT)," Electronics 2022.
3. L. Xiaoming, V. Sejdini, and H. Chowdhury, "Denial of service (dos) attack with udp flood," School of Computer Science, University of Windsor, Canada, 2010.
4. C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and Other Botnets,” Computer, vol. 50, no. 7, pp. 80–84, 2017.
5. [Tarak Nandy](https://www.researchgate.net/profile/Tarak-Nandy), [Mohd Yamani Idna Idris](https://www.researchgate.net/profile/Mohd-Idris-6), [Rafidah Md. Noor](https://www.researchgate.net/profile/Rafidah-Md-Noor) and [Sananda Bhattacharyya](https://www.researchgate.net/profile/Sananda-Bhattacharyya), "[Review on Security of Internet of Things Authentication Mechanism](https://www.researchgate.net/publication/336717897_Review_on_Security_of_Internet_of_Things_Authentication_Mechanism),"  [IEEE Access](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639), vol. 7, pp. 151054-151089, oct 2019.
6. Yinhao Xiao, Yizhen Jia, etc. "Edge Computing Security: State-of-The-Art and Challenges," Proceedings of the IEEE, vol. 107, no. 8, pp. 1608-1631, 2019.
7. R. Shanmugavadivu and N. Nagarajan, "Network intrusion detection system using fuzzy logic," Indian Journal of Computer Science and Engineering (IJCSE), vol. 2, no. 1, pp. 101–111, 2011.
8. M. Almseidin, M. Al-kasassbeh, and S. Kovacs, "Fuzzy rule interpolation and snmp-mib for emerging network abnormality," International Journal on Advanced Science, Engineering and Information Technology, vol. 9, no. 3, pp. 735–744, 2019.
9. M. Al-Kasassbeh, M. Almseidin, K. Alrfou, and S. Kovacs, "Detection of iot-botnet attacks using fuzzy rule interpolation," Journal of Intelligent & Fuzzy Systems, Vol 39, pp. 421–431, 2020.
10. M. Almseidin and S. Kovacs, "Intrusion detection mechanism using fuzzy rule interpolation," Journal of Theoretical and Applied Information Technology, vol. 96, no. 16, pp. 5473–5488, 2018.
11. B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, vol. 7, pp. 51 691–51 713, 2019.
12. S. Ghazanfar, F. Hussain, A. U. Rehman, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "Iot-flock: An open-source framework for iot traffic generation," in 2020 International Conference on Emerging Trends in Smart Technologies (ICETST). IEEE, 2020, pp. 1–6.
13. I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019, pp. 1–8.
14. M. Almseidin, J. Al-Sawwa, and M. Alkasassbeh, "Anomaly-based Intrusion Detection System Using Fuzzy Logic," in 2021 International Conference on Information Technology (ICIT), 2021, pp. 290-295
15. **Error! Hyperlink reference not valid.**J. Rabatel, S. Bringay, and P. Poncelet, "Fuzzy anomaly detection in monitoring sensor data," in Fuzzy Systems (FUZZ), 2010 IEEE International Conference on Fuzzy Systems, 2010, pp. 1-8.
16. M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," Computers & Security, vol. 86, pp. 147-167, 2019.
17. G. F. Scaranti, L. F. Carvalho, S. Barbon, and M. L. Proença, "Artificial Immune Systems and Fuzzy Logic to Detect Flooding Attacks in Software-defined networks," IEEE Access, vol. 8, pp. 100172-100184 2020.
18. M. E. Aminanto, H. Kim, K.-M. Kim, and K. Kim, "Another Fuzzy Anomaly Detection System Based on Ant Clustering Algorithm," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E100.A, pp. 176-183, 2017.
19. H. A. P. and K. K., "Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things," EURASIP Journal on Wireless Communications and Networking, vol. 2019, pp. 1-15, April 05 2019.
20. M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment," IEEE Access, vol. 8, pp. 83765-83781, 2020.
21. M. V. De Assis, A. H. Hamamoto, T. Abrão, and M. L. Proença, "A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks," IEEE Access, vol. 5, pp. 9485-9496, 2017.
22. M. Usman, V. Muthukkumarasamy, and X.-W. Wu, "Mobile agent-based cross-layer anomaly detection in smart home sensor networks using fuzzy logic," IEEE Transactions on Consumer Electronics, vol. 61, pp. 197-205, 2015.
23. H. S. Mondal, M. T. Hasan, M. B. Hossain, M. E. Rahaman, and R. Hasan, "Enhancing secure cloud computing environment by Detecting DDoS attack using fuzzy logic," in 2017 3rd International Conference on Electrical Information and Communication Technology (EICT), 2017, pp. 1-4.
24. [Hajar Moudoud](https://ieeexplore.ieee.org/author/37087093963); [Lyes Khoukhi](https://ieeexplore.ieee.org/author/37422168500); [Soumaya Cherkaoui](https://ieeexplore.ieee.org/author/37320995000), "Prediction and Detection of FDIA and DDoS Attacks in 5G Enabled IoT," [IEEE Network](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=65), Volume: 35, [Issue: 2](https://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=9387693), March/April 2021.
25. [Trong-Minh Hoang](https://www.researchgate.net/profile/Trong-Minh-Hoang), "A Study on Anomaly Data Traffic Detection Method for Wireless Sensor Networks," Intelligent Systems and Networks (pp.429-436), 2021.
26. **Error! Hyperlink reference not valid.Error! Hyperlink reference not valid.**Sharma, DK, Dhankhar, T, Agrawal, G, Singh, SK, Gupta, D, Nebhen, J and Razzak, Muhammad Imran, "Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks, Ad Hoc Networks", vol. 121, pp. 1-9, doi: 10.1016/j.adhoc.2021.102603.
27. [L Zhou](https://scholar.google.com.vn/citations?user=X5r6ILYAAAAJ&hl=en&oi=sra), [H Guo](https://scholar.google.com.vn/citations?user=UP80xZEAAAAJ&hl=en&oi=sra), [G Deng](https://scholar.google.com.vn/citations?user=NuzUkMEAAAAJ&hl=en&oi=sra)," [A fog computing based approach to DDoS mitigation in IIoT systems](https://www.sciencedirect.com/science/article/pii/S0167404818311349)," Computers & Security, vol. 85, pp. 51-62, 2019.
28. **Error! Hyperlink reference not valid.Error! Hyperlink reference not valid.**[S Myneni](https://scholar.google.com.vn/citations?user=wjndFcoAAAAJ&hl=en&oi=sra), [A Chowdhary](https://scholar.google.com.vn/citations?user=2Qji8kcAAAAJ&hl=en&oi=sra), [D Huang](https://scholar.google.com.vn/citations?user=Y_Bm7IwAAAAJ&hl=en&oi=sra), [A Alshamrani](https://scholar.google.com.vn/citations?user=7iRxITcAAAAJ&hl=en&oi=sra), "[SmartDefense: A distributed deep defense against DDoS attacks with edge computing](https://www.sciencedirect.com/science/article/pii/S1389128622000792)," Computer Networks, vol. 209 2022.
29. Lefoane, Moemedi; Ghafir, Ibrahim; Kabir, Sohag; Awan, Irfan U. "Machine Learning for Botnet Detection: An Optimized Feature Selection Approach," [ICFNDS 2021](https://dl.acm.org/doi/proceedings/10.1145/3508072).
30. Wan Nur Fatihah Wan Mohd Zaki, Raihana Syahirah Abdullah Warusia Yassin, Faizal M.A, Muhammad Safwan Rosli, "Constructing IoT Botnets Attack Pattern for Host-based and Network-based Platform," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 8, 2021.
31. Nicolas-Alin Stoian, "Machine Learning for Anomaly Detection in IoT networks: Malware analysis on the IoT-23 Data set," University of Twente.
32. [Imtiaz Ullah](https://ieeexplore.ieee.org/author/37086105502); [Qusay H. Mahmoud](https://ieeexplore.ieee.org/author/37267311100), "A Framework for Anomaly Detection in IoT Networks Using Conditional Generative Adversarial Networks," [IEEE Access](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639), vol. 9, pp. 165907-165931, 02 December 2021.
33. [Imtiaz Ullah](https://ieeexplore.ieee.org/author/37086105502); [Qusay H. Mahmoud](https://ieeexplore.ieee.org/author/37267311100) "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," [IEEE Access](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639), vol. 9, pp. 103906-103926, 01 July 2021.
34. Zhuotao Lian; Chunhua Su "Decentralized Federated Learning for Internet of Things Anomaly Detection", ASIA CCS '22: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, pp. 1249-1251, May 2022.