

Design of a Hybrid Framework for Detecting Attacks in Fog-based IoT Architecture using Deep Learning

Navnath B. Pokale¹, Pooja Sharma² and Deepak T. Mane³

¹Research Scholar, Dept. of Computer Engineering, School of Engineering and Technology, D. Y. Patil University, Ambi, Pune, India 410507

Email: nbpokale77@gmail.com

²Guide, Dept. of Computer Engineering, School of Engineering and Technology, D. Y. Patil University, Ambi, Pune, India 410507

Email: poojasharma861984@gmail.com

³Co-guide, Dept. of Computer Engineering, Vishwakarma Institute of Technology, Pune, India

Email: dtmane@gmail.com

Abstract— IoT-Fog computing offers a broad variety of services for IoT-based end-systems. End IoT devices communicate with cloud nodes and fog nodes to administer client tasks. During the data collection process between the fog and cloud layers, IoT endpoints are more likely to be compromised by critical attacks such as DDoS and other security threats. It is necessary to detect these network vulnerabilities early on. By extracting features and placing the danger in the network, DL is crucial in predicting end-user behavior. Due to the limited processing power and less storage, Deep Learning algorithms cannot be directly implemented on IoT devices. In this article, we present a three stage Deep Hybrid Detection Model for Attack Detection in IoT-Fog Architecture. Enhanced Z-score normalization based data preparation will be carried out in the beginning. On the basis of preprocessed data, features such as IG, raw data, entropy, and enhanced MI are extracted in the second step. The collected characteristics are used as an input to hybrid classifiers called DBN and optimized DeepMaxout in the third stage to classify the assaults based on the input dataset. A hybrid optimization model known as the BMJFO (Blue Monkey Jelly Fish Optimization) algorithm is presented for the best DeepMaxout training. The suggested model produced increased accuracy, precision, sensitivity, and specificity. The suggested model produced superior accuracy, precision, sensitivity, and specificity of 95.80%, 94.94%, 96.38%, and 97.94%, respectively.

Index Terms— IoT, Fog computing, DDoS, DL, z-score, MI, DeepMaxout, DBN, BMJFO

I. INTRODUCTION

The term "Internet of Things" (IoT) refers to the huge network of interconnected physical devices, objects, and systems that are integrated with sensors, software, and networking capabilities, enabling them to gather and exchange data over the internet. The Internet of Things (IoT) is regarded as a rapidly evolving paradigm in computing history. It is a rapidly expanding network that has the ability to alter the lives of people and is the subsequent significant step forward in the evolution of internet technology. IoT has evolved tremendously in various technology domains during the last few years [1]. IoT applications are growing tremendously. It is estimated that by 2025, 90 billion devices will be connected to Internet. Its presence is felt in all the domains. Some of the

applications of IoT are smart home, smart industry, smart farming, smart city, smart healthcare, smart vehicles, smart wearable, and smart grid. It is also used in defense industry. The services provided by IoT applications are of great benefit to human existence, but they may come at a high price in terms of the individual's privacy and security [2].

With the increasing IoT devices, there are a numerous security problems. In an IoT network, the security requirements generally appear as network anomalies [3] especially when there is a deviation from the usual network data flow. Such anomalous network flows include attacks like DDoS and probing attacks. A larger number of compromised network nodes or systems that are under the control of bad actors make up a botnet. A number of attacks are carried out via these nodes or systems [4].

IoT devices are brought closer to the processing and storage resources by using fog computing. Fog computing emerges in IoT applications as the necessity for quick response activities rises [5]. A decentralized network called fog computing [6] is sensitive to the context of data related to data sources, such as reaction time, location, resources spread by the services, etc. At the network's edge node, it is made accessible physically or electronically. IoT security is challenging due to the variety, complexity, lack of hardware resources, and accessibility of IoT systems on a global scale. Researchers used ML techniques including DT, RF, SVM, Bayesian network, and K-Means to discover network attacks. Researchers used ML techniques including DT, RF, SVM, Bayesian network, and K-Means to discover network attacks. Both valid and malicious traffic is used to create the trained models for machine learning techniques. Based on the learning process, these techniques are categorized as supervised, unsupervised, or semi-supervised. Due to its numerous processing stages [7]. For vast volumes of data, DL is recommended over ML. For a node's behavioral update, the cloud receives a binary classification of normal and abnormal activity as well as multi-label categorization supplied by DL, which has been used in classifying several assaults with a high detection rate. The idea of fog computing is put out to assist cloud computing in handling data for Internet of Things applications. Nevertheless, fog computing has several challenges that must be solved, including those related to storage, security, and privacy. So we have proposed "Design and Development of a Framework for Detecting Attacks in Fog-Based IoT Architecture using Deep Learning" with following contributions

1. The preprocessing of input data using z-score normalization. Feature extraction is done using enhanced Mutual Information.
2. A hybrid model is used to classify output using DBN and enhanced DeepMaxout algorithms.
3. DeepMaxout is optimized with BMJFO.

II. RELATED WORK

A VCDL approach was used in 2020 by Bhuvaneswari Amma N.G. and S. Selvakumar [8] to provide an anomaly detection framework in a fog environment. The anomaly detection approach may be scalable if the communication could be routed among the nodes inside the fog layer for processing. The VCDL method, which spread the IoT traffic training and carried out computations in the fog nodes, successfully caught this. The training settings were given by the master node of the fog layer. Before being transferred to the cloud for attack mitigation, IoT traffic is further identified by the recommended anomaly identification system as either regular or attack traffic.

In 2020, Ahmed Samy et al. [1] created a thorough architecture for detecting attacks that employs distributed, dependable, and high detection rates to discover various IoT cyber-attacks. A fog node attack detection technique may be designed using the suggested scheme's distributed architecture, high computing power, and closeness to edge devices. In order to identify the best DL model, six DL designs were tested.

DI-ADS was proposed in 2022 by Surya Pavan Kumar Gudla et al. [9] for IoT applications that depend on fog. The system mainly use a DL to recognize DDoS assaults on the network. The DL is embedded in the computation module of the fog node, which anticipates the eventual IoT device behavior. To choose the best DLM model for the fog layer, the efficacy of DNMLP, LSTM, and more established ML models like SVM, LR, k-NN, and RF are compared. In the recommended approach, DNMLP was taken into consideration for implementation at the fog layer since it outperforms nature at identifying DDoS assaults.

DL models-based fog-based IoT attack prognostication technique was proposed by Surya Pavan Kumar Gudla et al. [2] in 2022. The network is divided into three tiers: a secure fog tier, a smart sensing tier, and a cloud tier. Then, a variety of DL models, including LSTM, DNMLP, Bi-LSTM, CNN + LSTM, GRU, and HEM, were assessed in order to accurately forecast which model will be deployed at the fog nodes. In tests employing the relevant datasets, the LSTM classifier outperformed nature in classification tasks, achieving performance accuracies of 99.12%, 99.88%, 94.11%, and 99.70%.

A real-time FLFSIoT was proposed for 2020 by Syed Rameem Zahra and Mohammad Ahsan Chishti [10]. Fuzzy logic is utilized in FLFSIoT to both reduce the danger of an edge node joining a single crisp cluster and to identify a variety of traditional assaults. By lowering latency and other problems, the Fog-based IoT architecture has been

leveraged to make FLFSIoT inherently more secure than cloud-supported IoT. As a consequence, in order to create a comprehensive solution to the IoT security dilemma, our study leverages the advantages of fog computing and fuzzy logs. When FLFSIoT's efficacy was examined in relation to DDoS and cooperative assaults, it was discovered that FLFSIoT's findings were more precise than those of the prior benchmarks.

A GLSF2IoT technique based on the notion of "zero trust," or the idea that everything should be treated with suspicion, was suggested in 2022 by Syed Rameem Zahra and Mohammad Ahsan Chishti [11]. The Fog-IoT architecture of GLSF2 IoT makes it fundamentally superior than cloud-IoT, even if Fuzzy Logic was previously employed to reduce uncertainty. In order to stop the malicious behavior from spreading to other devices, GLSF2IoT instantly limits network access to the IoT device that started the harmful activity.

A 2021 architecture for IoT networks that can identify abnormalities on the fog layer was put out by Deepak Kumar Sharma et al. [12]. The strategy was typical of statistical algorithms because it depended on the CRPS measure and only employed one variable. They had therefore provided a technique for utilizing several variables and demonstrated why it was essential in a heterogeneous system like the IoT.

A distributed ensemble model aided IDS using fog computing was created in 2021 by Prabhat Kumar et al. [13] by merging first-level individual learners from KNN, NB, and Gaussian XGBoost. For the final prediction at the second level, RF used the first-level prediction results. The effectiveness of the proposed methodology was examined in this study using the UNSW-NB15 dataset and a real IoT-based dataset, DS2OS. In Table 1, we have presented the techniques, advantages, and disadvantages.

III. PROBLEM STATEMENT

IoT offers many advantages, but it also faces three major problems: data collection, data transport, and data security. As there were more linked devices to the Internet, authorization became a significant issue in the IoT system. Some of the major difficulties in the work under study are the ones listed below: It is required to compare the recommended attack detection in LSTM model to unsupervised DL models in a distributed computing environment with different datasets. It is necessary to enhance attack prediction using multiclass classification. The fundamental concern with the VCDL technique is the problem of class imbalance. Passive attacks are more difficult to identify. It is required to integrate multiclass classification with updated datasets in order to identify particular assaults. It is necessary to develop a prototype that validates the formal security properties of the entire architecture in order to increase IoT security. To account for hardware assaults, work must be increased. Real-time anomaly detection is difficult.

A. Motivation

The use and expansion of the Internet of Things (IoT) have accelerated recently. The security of these systems grows in importance as more devices are networked. Fog computing has evolved as a way to deal with latency, bandwidth, and privacy challenges in IoT applications by extending cloud computing capabilities to the edge of the network. IoT systems based on fog can expand to dozens or even millions of units and be quite complicated. Given the size and dynamic nature of these systems, conventional security measures might not be enough. Neural networks and other deep learning techniques have shown they can manage complicated and high-dimensional data, making them a potential method for IoT security analytics. Fog-based IoT systems have more attack vectors and vulnerabilities due to their scattered nature. Fog networks are vulnerable to several forms of assaults, including malware infections, unauthorized access, data breaches, and denial-of-service (DoS) attacks, due to the sheer quantity and variety of devices, as well as the varied communication protocols and the dynamic nature of fog networks.

In IoT systems, prompt identification and reaction to security risks are essential. Traditional security measures frequently rely on rule-based strategies or signature-based detection, both of which may be ineffective against fresh and developing threat vectors. Real-time pattern learning and anomaly detection capabilities of deep learning algorithms make it possible to identify and mitigate assaults early on.

IV. PROPOSED ATTACK DETECTION FRAMEWORK

A. Fog-Based IoT Architecture

In a typical IoT architecture, data is routed from the edge layer to higher levels using smart gateway devices. The distance between the cloud and the edge layer makes data analysis time-consuming and subject to delays [1]. Hence, this approach is not appropriate for handling sensitive information that requires a prompt response. Fog computing is used to address these issues by bringing the cloud closer to the data sources. CISCO proposed fog computing in 2012 to address the limitations of cloud computing [6]. Bonomi et al. defined fog computing as follows – "Fog Computing is a highly virtualized platform that provides compute, storage, and networking services

between end devices and traditional Cloud Computing Data Centers, typically, but not exclusively located at the edge of network”. Fog architecture is divided into three layers i. e. edge layer, fog layer and cloud layer as shown in figure1. Large data sizes are generated by this layer jfrom many sources and applications. Between the edge and the cloud layer lies an intermediary layer called the fog layer. Each domain in the fog layer incorporates virtualized fog servers, routers, minimal data centers, applications, and services. The fog layer is separated into multiple connected domains. The cloud layer, which is the core layer and includes high-performance servers and storage devices, is the layer above.

There are several attack detection methods that have been developed for the aim of detecting attacks in IoT-Fog computing. However, gathering pertinent information is a challenging procedure because of IoT device constraints such dispersion, low latency, resource limitations, and scalability. To address this issue, an efficient assault detection method dubbed as a Hybrid Framework for Detecting Attacks in Fog- Based IoT Architecture using Deep Learning. It is a 3 stage framework.

TABLE 1 TECHNIQUES, ADVANTAGES, AND DISADVANTAGES

Author [Citation]	Technique	Advantages	Disadvantages
Selvakumar S., Bhuvaneswari Amma, and N.G. [8]	VCDL strategy	High precision and little error	Problem of class disparity.
Ahmed Samy et al [1]	LSTM algorithm	High accuracy	The proposed attack detection must be tested against unsupervised DL models using a variety of datasets in a distributed computing environment.
Surya Pavan Kumar Gudla et al.[9]	DI-ADS	Precision, recall F1-score, and accuracy are high	It is required to integrate multiclass classification with up-to-date information in order to identify particular assaults.
Surya Pavan Kumar Gudla et al [2]	LSTMDL	Accuracy is high	It is necessary to enhance attack prediction using multiclass classification.
Syed Rameem Zahra and Mohammad Ahsan Chishti [10]	FLFSIoT	Attack detection accuracy is high	Passive attacks are more difficult to identify.
Syed Rameem Zahra and Mohammad Ahsan Chishti [11]	Generic and Lightweight Security framework	Higher accuracy	To take hardware assaults into consideration, work must be broadened.
Deepak Kumar Sharma et al. [12]	Anomaly Detection model	Latency is low	Real-time anomaly detection is difficult.
Prabhat Kumar et al. [13]	Distributed ensemble design	Accuracy is higher	It is necessary to develop a prototype that verifies the formal protocols for IoT security in order to enhance

1. Preprocessing using Z-score

Preprocessing is the first step, during which input data is preprocessed using the Z-score normalization procedure. "Z-score normalization" is a normalization method based on the mean and standard deviation of the input data, and it is outlined in equation (1). This approach [14] is very beneficial if the input data's actual lowest and highest values are unknown.

$$Z - score = \frac{I^d - \mu}{\sigma} \quad (1)$$

$$I_p^d = Z - score_{new} = \frac{I^d - MAD}{QD} \quad (2)$$

Entropy, Improved MI, and raw data, are extracted from the preprocessed data in the second stage, which is known as feature extraction. The quantity of redundant and unnecessary data in the input preprocessed data set is decreased with the aid of feature extraction.

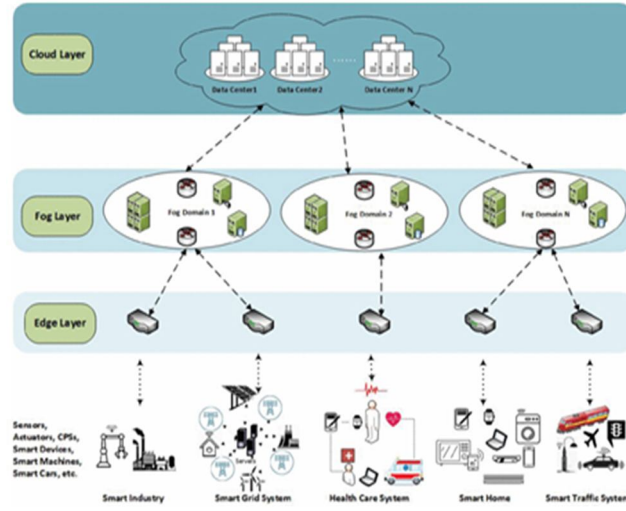


Fig. 1 IoT fog architecture [1]

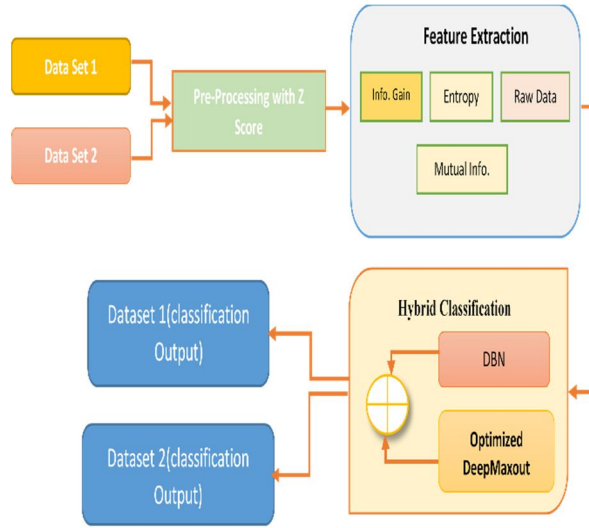


Figure 2 Architecture Proposed attack detection Framework

Information Gain: IG determines the drop in entropy or surprise by splitting a preprocessed dataset matching to a particular value of a random variable. A lower entropy in a collection or collections of samples, as indicated by a greater IG, means that there will be less surprise. For instance, we may decide to determine the impact on purity by dividing a preprocessed dataset by a random variable with such a range of values [15]. We can calculate it using the following equation.

$$IG(I_p^d, a) = H(I_p^d) - H(I_p^d | a) \quad (3)$$

Entropy: Entropy is a measure of the expected amount of information that is transmitted by determining the outcome of a random experiment. It is represented by the following equation.

$$H(X) = H(p_1, \dots, p_n) = -\sum_{i=1}^n p_i \log_2 p_i \quad (4)$$

Mutual Information: The word "MI" refers to the quantity of information that may be obtained from a certain random variable given another. It is obtained by the following equation.

$$IMI(X; Y) = [H(X) - H(X | Y)] + \frac{1}{2} [B_x \cdot E(u) + B_y \cdot E(v)]$$

2. Attack Detection

Attack detection in this step involves feeding extracted characteristics into a hybrid classifier, such as Deep max out and DBN that have been improved. We employ a hybrid classification strategy to attain fairly high accuracy in contrast to core algorithms without sacrificing the interpretability of learning outcomes. A novel hybrid optimization approach called Blue Monkey Updated Jelly Fish Optimization (BMUJFO) is developed for boosting the Deep Max out classifier's performance and classification accuracy. This algorithm combines the BMO [16] and JFO algorithm [17].

DBN model: DBN is a subtype of DNN that consists of layers of dependent variables connected only between adjacent layers, not between individual units within each layer. DBN is used to tackle issues with conventional neural networks in deep layered networks. CNN or deep feed forward networks are replaced by DBN in more complicated environments. The benefit of them is that they require less calculation. Because computing complexity rises in proportion to the number of layers, as opposed to feed-forward neural networks, it is less susceptible to the vanishing gradients problem [18].

Optimized DeepMaxout: Using the maxout unit in a feed-forward architecture, the maxout approach is a novel activation strategy. The output of several linear functions can be entered into the maxout unit, which returns the highest value supplied in the equation.

Here $G_{ij} = F^T w_{ij} + s_{ij}$, $w \in C^{d \times m \times k}$, $s \in C^{m \times k}$ tends to the learning variables, w tends to weight function optimized by BMJFO, s tends to the bias of deep maxout. The performance of the maxout network improves when it can distinguish between words specified in convex sets. The Maxout Unit generalizes both the ReLU and the leaky ReLU functions. It refers to a piecewise linear method that uses dropout to merge the greatest input feature. The maximum preactivations value is used in neural networks as the maximum activation [19].

$$H_i(F) = \max_{j \in [1, k]} G_{ij} \quad (4)$$

To reach the final detected result, the improved DeepMaxout classifier and DBN classifier's predicted scores were averaged.

BMJFO algorithm for optimal DeepMaxout weight tuning (*w): This section discusses the mathematical model and the theory underlying the suggested BMUJFO approach. As shown by equation, the main objective of this study is to decrease the discrepancy between expected and actual production.). Here, the DeepMaxout weight is provided as an input solution to the proposed BMUJFO to obtain the optimal weight .

$$Obj = Min(err) \quad (5)$$

Proposed BMJFO algorithm: BMJFO is a ground-breaking meta-heuristic algorithmic optimization that is based on how well blue monkey swarms function in nature. The BMUJFO algorithm and its mathematical model are presented here.

Group formation: The BMJFO model simulates the actions of blue monkeys. Each set of monkeys had to travel the search area in order to mimic these interactions. Stronger and more mobile monkeys start looking for food sources outside the normal field of their vision when they are divided into groups. Cercopithecus mitis seems to engage with its young males seldom or not at all. Due of its territorial tendency, juvenile male cercopithecus mitis should venture outside as soon as feasible. They'll be tested by an alpha male from another household. If they are able to overcome, they will become family leaders who can give young men food, housing, and socialization. In blue monkey groups, there are frequently more females and young present than males.

Position update: The behavior of updating each blue monkey's position depending on the new location in each group is defined by continuity equations, where monkey power rate, leader weight, monkey weight, and random variable tend to be constants.

$$Rate = (0.7 * Rate_i) + (M_{lead} - M_i) * rand * (w_{best} - w_i) \quad (6)$$

$$w_{i+1} = w_i + Rate_{i+1} * rand \quad (7)$$

$$w_i(t+1) = w_i(t) + \gamma * rand(0,1) * (Ub - Lb) \quad (8)$$

$$(16)$$

$$w_i = \frac{\gamma * (Ub - Lb) - (0.7 * Rate_i) * \frac{-1}{rand}}{(M_{lead} - M_i) * rand * w_{best}} \quad (9)$$

Algorithm 1: Pseudocode of proposed BMJFO algorithm for optimal DeepMaxout weight (w) tuning
Input: DeepMaxout weight (w), Output: Optimal DeepMaxout weight (w^*)
Initialization of blue monkey as well as population of children as: $b_i (i = 1, \dots, n)$
Randomly distribute the blue monkey into group G while overall children in a single group
Compute child and overall blue monkey fitness in every group
for each group, worst and best fitness value is selected and stored it in a present best
while best fitness is selected by child
$t = 1$
while ($t \leq Max_{iter}$)
Swap each group worst fitness by child group best fitness
Update blue monkey position using eq. (17) as per BMUJFO model
Update child position using eq. (20) as per BMUJFO model
Update blue monkey and children fitness and update the present best
If new best is better when compared to present best then
present best=new best
$t = t + 1$
end while

V. CONCLUSION

In this study, a three stage process for a Deep Hybrid Detection Model for Attack Detection in IoT-Fog Architecture is provided. The first stage would involve enhanced Z-score normalization based data preparation. The second step involves extracting characteristics such as IG, raw data, entropy, and enhanced MI from the preprocessed data. The third step introduces a hybrid attack detection model by feeding the retrieved features to hybrid classifiers dubbed optimized DeepMaxout and DBN to categorize the assaults based on the input dataset. BMUJFO (Blue Monkey Updated Jelly Fish Optimization) method was created as a hybrid optimization model for DeepMaxout training.

REFERENCES

- [1] Samy, H. Yu, and H. Zhang, "Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning," IEEE Access, vol. 8, pp. 74571–74585, 2020, doi: 10.1109/ACCESS.2020.2988854.
- [2] S. P. K. Gudla, S. K. Bhoi, S. R. Nayak, K. K. Singh, A. Verma, and I. Izonin, "A Deep Intelligent Attack Detection Framework for Fog-Based IoT Systems," Comput. Intell. Neurosci., vol. 2022, pp. 1–25, Dec. 2022, doi: 10.1155/2022/6967938.
- [3] D. K. K. Reddy, H. S. Behera, J. Nayak, B. Naik, U. Ghosh, and P. K. Sharma, "Exact greedy algorithm based split finding approach for intrusion detection in fog-enabled IoT environment," J. Inf. Secur. Appl., vol. 60, Aug. 2021, doi: 10.1016/j.jisa.2021.102866.
- [4] C. Koliass, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer (Long. Beach. Calif.), vol. 50, no. 7, 2017, doi: 10.1109/MC.2017.201.
- [5] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," MCC'12 - Proc. 1st ACM Mob. Cloud Comput. Work., pp. 13–15, 2012, doi: 10.1145/2342509.2342513.
- [6] X. Li, Y. Liu, H. Ji, H. Zhang, and V. C. M. Leung, "Optimizing resources allocation for fog computing-based internet of things networks," IEEE Access, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2917557.
- [7] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," IEEE Access, vol. 10, pp. 121173–121192, 2022, doi: 10.1109/ACCESS.2022.3220622.
- [8] B. A. Bhuvaneswari and S. S., "Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment," Futur. Gener. Comput. Syst., vol. 113, pp. 255–265, Dec. 2020, doi: 10.1016/j.future.2020.07.020.
- [9] S. P. K. Gudla, S. K. Bhoi, S. R. Nayak, and A. Verma, "DI-ADS: A Deep Intelligent Distributed Denial of Service Attack Detection Scheme for Fog-Based IoT Applications," Math. Probl. Eng., vol. 2022, 2022, doi: 10.1155/2022/3747302.
- [10] S. R. Zahra and M. A. Chishti, "Fuzzy logic and Fog based Secure Architecture for Internet of Things (FLFSIoT)," J. Ambient Intell. Humaniz. Comput., May 2020, doi: 10.1007/s12652-020-02128-2.
- [11] S. R. Zahra and M. A. Chishti, "A generic and lightweight security mechanism for detecting malicious behavior in the uncertain Internet of Things using fuzzy logic- and fog-based approach," Neural Comput. Appl., vol. 34, no. 9, pp. 6927–6952, May 2022, doi: 10.1007/s00521-021-06823-9.
- [12] D. K. Sharma et al., "Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks," Ad Hoc Networks, vol. 121, Oct. 2021, doi: 10.1016/j.adhoc.2021.102603.

- [13] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 10, pp. 9555–9572, Oct. 2021, doi: 10.1007/s12652-020-02696-3.
- [14] H. 1, T. Wahyuningsih, and E. Rahwanto, "Comparison of Min-Max normalization and Z-Score Normalization in the K-nearest neighbor (kNN) Algorithm to Test the Accuracy of Types of Breast Cancer." [Online]. Available: <http://archive.ics.uci.edu/ml>.
- [15] R. Koprowski and K. R. Foster, "Machine learning and medicine: book review and commentary," *Biomed. Eng. Online*, vol. 17, no. 1, 2018, doi: 10.1186/s12938-018-0449-9.
- [16] M. Mahmood and B. Al-Khateeb, "The blue monkey: A new nature inspired metaheuristic optimization algorithm," *Period. Eng. Nat. Sci.*, vol. 7, no. 3, pp. 1054–1066, Sep. 2019, doi: 10.21533/pen.v7i3.621.
- [17] J. S. Chou and D. N. Truong, "A novel metaheuristic optimizer inspired by behavior of jellyfish in ocean," *Appl. Math. Comput.*, vol. 389, Jan. 2021, doi: 10.1016/j.amc.2020.125535.
- [18] Y. Bengio, P. Lamblin, H. Larochelle, Y. Bengio, and D. Popovici, "Greedy layer-wise training of deep networks Parsing View project Optical Neural Network View project Greedy Layer-Wise Training of Deep Networks Département d'Informatique et Recherche Opérationnelle," 2007. [Online]. Available: <https://www.researchgate.net/publication/200744514>
- [19] I. J. Goodfellow, D. Warde-Farley, M. Mirza, A. Courville, and Y. Bengio, "Maxout Networks," Feb. 2013, [Online]. Available: <http://arxiv.org/abs/1302.4389Y>.
- [20] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, et al., "Machine learning and deep learning methods for cybersecurity", *IEEE Access*, vol. 6, pp. 35365-35381, 2018.
- [21] A. Diro and N. Chilamkurti, "Leveraging LSTM networks for attack detection in Fog-to-Things communications", *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 124-130, Sep. 2018.
- [22] M. Ali Al-Garadi, A. Mohamed, A. Al-Ali, X. Du and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security", *CoRR*, vol. abs/1807.11023, 2018.
- [23] P. Torres, C. Catania, S. Garcia and C. G. Garino, "An analysis of recurrent neural networks for botnet detection behavior", *Proc. IEEE Biennial Congr. Argentina (ARGENCON)*, pp. 1-6, Jun. 2016.
- [24] Y. Fu, F. Lou, F. Meng, Z. Tian, H. Zhang and F. Jiang, "An intelligent network attack detection method based on RNN", *Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC)*, pp. 483-489, Jun. 2018.
- [25] D. Lavrova, D. Zegzhda and A. Yarmak, "Using GRU neural network for cyber-attack detection in automated process control systems", *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, pp. 1-3, Jun. 2019.
- [26] M. P. Maharani, P. Tobianto Daely, J. M. Lee and D. -S. Kim, "Attack Detection in Fog Layer for IIoT Based on Machine Learning Approach," 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2020, pp. 1880-1882, doi: 10.1109/ICTC49870.2020.9289380.
- [27] K. F. Hassan and M. E. Manaa, "Detecting Distributed Denial of Service Attacks in Internet of Things Networks Using Machine Learning in Fog Computing," 2022 5th International Conference on Engineering Technology and its Applications (IICETA), Al-Najaf, Iraq, 2022, pp. 323-328, doi: 10.1109/IICETA54559.2022.9888699.