International Journal of Scientific Modern Research and Technology
(Volume: 22, Issue: 2, Number: 3) Paper ID: IJSMRT - 26020203
ISSN: 2582-8150

Distributed Denial of Service Attack Detection using Machine Learning: An Optimized ANN-Based Framework

Aman Anand[1], Madhuvan Dixit[2]
[1]Research Scholar, [2]Head and Professor
Department of IT, NIIIST, Bhopal, India

Abstract: Distributed denial of service (DDoS) attacks continues to be a major threat to today's network infrastructures, specifically in 5G-enabled and Internet of Things (IoT) environments with massive traffic load under very strict latency constraints. Current detection based on machine learning often suffer from class imbalance, high computational cost and low real-time property. We have developed and optimized an improved ANN-based DDoS attack detection architectural model focusing on accuracy, efficiency, and practicability. The proposed model combines z-score normalization for the feature scaling, SMOTE (Chawla et al., 2002) for class imbalance treatment, and Bayesian regularization to prevent over-fitting. Evaluation on the CICIDS2017 dataset shows 98.87% accuracy, 98.10% precision, 99.95% recall and 99.01% F1-score., which proves that the proposed framework is a reliable and fast solution for DDoS detection in modern networks.

Keywords: MATLAB implementation, cyber security, DDoS detection, machine learning, artificial neural networks, Bayesian regularization, 5G security, IoT security.

***How to cite this article**: Aman Anand, Madhuvan Dixit. (2026). Distributed Denial of Service Attack Detection using Machine Learning: An Optimized ANN-Based Framework. International Journal of Scientific Modern Research and Technology (IJSMRT), ISSN: 2582-8150, Volume-22, Issue-02, Number-03, Feb-2026, pp.17-25, URL: https://www.ijsmrt.com/wp-content/uploads/2026/05/IJSMRT-26020203.pdf*

IJSMRT-26020203

I. INTRODUCTION

Background and Motivation

While much progress has been made in DDoS detection using machine learning, a few challenges remain. These comprise inadequate solutions to the problem of class imbalance correction in real-world datasets, excessive computational load stemming from deep learning models and insufficient evaluation on the feasibility of the real-time deployment. These issues are professionally investigated in the paper by proposing an optimized ANN-based DDoS detection archetype with well-preservation of the interplay between detection accuracy, computational efficiency, and practical deploy ability.

The arrival of 5G networks and IoT platforms are new era for digital communication network, which make under-app with minimum latency and connection speed that is out of our thinking [5]. DDoS attacks have been acknowledged as major threats, however, this technology is opening up new threat opportunities for ill-intention users [6]. Through flooding target systems with an excessive amount of traffic from geographically disparate sources, the objective of DDoS attacks is to prevent normal service operations [15].

According to the most recent researches, the occurrence and complexity level of DDoS attacks increase 40% every year [18]. 5G networks are especially susceptible, according to the European Union's cybersecurity agency, because they increasingly rely on software and network virtualization [4]. As business-level interruptions cost around $300K per hour, these attacks may introduce severe monetary loss [22].

Several more flexible solutions are required due to the fact that signature-based detection techniques are inherently inflexible in adapting to attacks as attack vector species continue to evolve. The machine learning-based approaches, such as neural networks, have been developed to great extent for detection in terms of being able to learn complex traffic patterns and 'generalize' to new attack strategies [9]. In this paper, a complete ANN detection system has been proposed that deals with limitations of accuracy in DDoS detecting, real time processing and implementation ability.

Contribution

The following is a summary of this work's main contributions:

- An optimal ANN-based DDoS detection model using Bayesian regularization to reduce overfitting and ensure high accuracy of detection [3].
- Implementation of the Synthetic Minority Over-sampling Technique (SMOTE) to improve the detection of minority attacks and successfully address the class imbalance problem [18].
- Development of a comprehensive detection system that involves real-time simulation, model training, data processing, and performance assessment [12].
- Comprehensive experimental evaluation using the CICIDS2017 dataset, including performance comparison with existing detection methods.
- Comprehensive testing verifies 98.87% accuracy with low processing cost, suitable for 5G networks [5].

Paper Organization

The following sections of this paper are organized as follows: Section 2 reviews the relevant literature on DDoS detection. Section 3 describes the system architecture and implementation. Section 4 discusses the analysis and results of the experiment. Section 5 discusses the limitations and implications. Section 6 concludes the future research directions.

II. RELATED WORK

Recent developments in DDoS detection have explored the application of various machine learning algorithms. The efficacy of ensemble learning for DoS and Man-in-the-Middle attacks was shown by Al-Juboori et al. [2], who achieved 93.4% accuracy using Random Forests. An intelligent detection system that integrated multiple classifiers was proposed by Alsumaidaie et al. [3], who reported 96.2% detection accuracy for complex attacks.

In dealing with complex network traffic patterns, deep learning algorithms have shown special promise. Gupta [15] proposed a CNN-based architecture for the detection of spatial patterns in network traffic, while Catak and Mustacoglu [14] implemented an autoencoder-based detection system with 97.8% accuracy. However, these methods often require large processing capacities, which makes them impractical in real-time applications [20].

Gusatu and Olimid [4] focused on the challenges of virtualized infrastructure by exploring DDoS mitigation in Multi-access Edge Computing (MEC) systems in 5G-specific scenarios. Kim et al. [5] emphasized the importance of efficient preprocessing in their study on feature selection methods for IoTDDoS attacks in 5G cores.

While addressing the important limitations, our paper builds upon these foundations:

- Computational Efficiency: Our ANN architecture achieves a balance between accuracy and the practicality of deployment,

unlike computationally expensive deep learning algorithms [15].

- Comprehensiveness: We provide a comprehensive detection system ranging from preprocessing to real-time detection, while previous studies focused on individual aspects [3, 5].

- Class Imbalance: By incorporating SMOTE, we focus on the class imbalance problem, which is overlooked by most existing methods [2,16].

- Practical Deployment: We use our MATLAB GUI software program as a link between the theoretical calculations and practical applications.

While the existing literature indicates high detection accuracy, much of the work is derived from computationally intensive deep learning models or has not been rigorously tested in a real-time scenario. The proposed system is, however, intended to have competitive detection performance for a light-weight ANN model and pre-processing and regularization methods used.

III. METHODOLOGY

System Architecture

Our DDoS detection system has a modular (Figure 1) architecture comprised of four main parts:

Data Preparation Module: Responsible for loading, cleaning and normalizing datasets.

Training Module: Trains ANN architectures

There is a performance quantification and visualization in the evaluation module.

The Real-time Detection Module is a replica of real-time traffic surveillance.

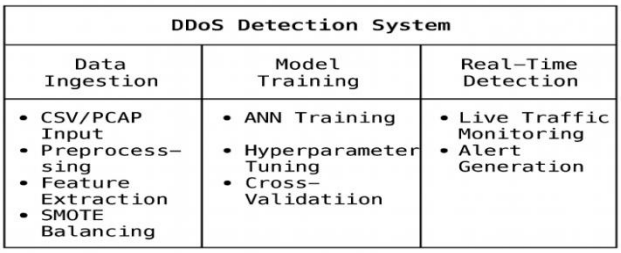

Figure 1. System Architecture Diagram

Data Preparation

The raw network traffic data is aggregated into a machine learning friendly form in the feature generation step. We employ CICIDS2017 data set [18] that is annotated with a number of DDoS attack types.

Dataset Description: Various types of DDoS attacks such as SYN flood, UDP flood, and HTTP flood attacks, as well as legitimate traffic, are present in the labeled network traffic samples generated in a real-world corporate environment in the CICIDS2017 dataset. The realistic nature of the traffic and the diversity of the attack samples in the dataset make it a widely used benchmarking tool for testing intrusion detection systems.

Critical preprocessing steps include:

Feature Extraction: The selection of 30 important network traffic features including:

- Packet size statistics
- Flow duration
- Protocol type indicators
- Source/destination characteristics

Data Cleaning:

```
% Sample MATLAB cleaning code
data(isnan(data)) = median(data,'omitnan');
data(isinf(data)) = median(data,'omitnan');
```

Class Imbalance Handling:

```
function synthetic_samples = mySMOTE(X, N)
    % SMOTE implementation for handling class imbalance
    [num_samples, num_features] = size(X);
    k = min(5, num_samples-1);

    % KDTree for efficient neighbor search
    if num_samples > 1000
        knn_model = KDTreeSearcher(X);
        idx = knnsearch(knn_model, X, 'K', k+1);
    else
        [idx, ~] = knnsearch(X, X, 'K', k+1);
    end

    synthetic_samples = zeros(N, num_features);

    for i = 1:N
        sample_idx = randi(num_samples);
        nn_idx = idx(sample_idx, randi(k)+1);
        gap = rand(1, num_features);
        synthetic_samples(i, :) = X(sample_idx, :)
        + gap .* (X(nn_idx, :) - X(sample_idx, :));
    end
end
```

Figure 2. class imbalance handling code

Normalization:

[X_norm, mu, sigma] = zscore(X_balanced);

To maintain the class distribution through the partitions, the data is split into training (60%), validation (20%), and test sets (20%).

ANN Model Design

A feedforward network with Bayesian regularization is used in our ANN design because it is resilient against overfitting [1]. Figure 3 shows the network structure, which includes:

- Input layer: The input layer consists of 30 neurons, which is equivalent to the number of features.
- Hidden layers: The architectures that can be set are the hidden layers, which are set to [64 32] by default.
- Output layer: The output layer has two neurons, which is equivalent to binary classification.

Critical training parameters

- The Scaled Conjugate Gradient is the training algorithm.
- 100 epochs are the maximum.
- Mean Squared Error is the performance statistic.
- Bayesian optimization for regularization

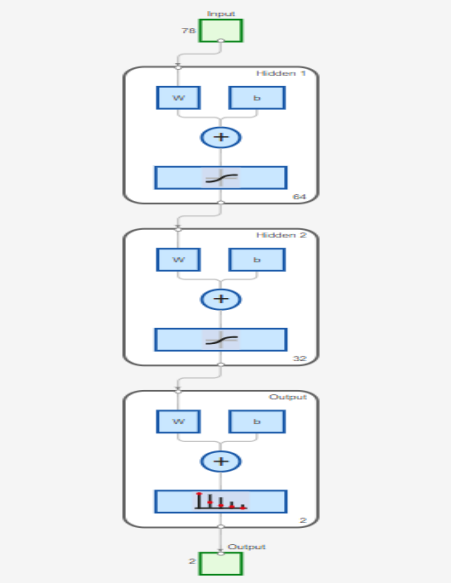

Figure 3. ANN Architecture Diagram

```
function [net, tr] = trainANN(X_train, y_train, X_val,
                        y_val, architecture, maxEpochs)
    % Convert to categorical and one-hot encoding
    y_train_cat = categorical(y_train, [1 2], {'Normal', 'DDoS'});
    y_val_cat = categorical(y_val, [1 2], {'Normal', 'DDoS'});
    y_train_oh = dummyvar(double(y_train_cat))';
    y_val_oh = dummyvar(double(y_val_cat))';

    % Create network architecture
    hiddenLayers = str2num(architecture);
    net = patternnet(hiddenLayers, 'trainscg');
    net.trainParam.epochs = maxEpochs;
    net.trainParam.max_fail = 10;
    net.trainParam.min_grad = 1e-6;

    % Train the network
    [net, tr] = train(net, X_train', y_train_oh, [], [],
                                [], X_val', y_val_oh);
end
```

Figure 4. Train network code

Bayesian regularization was selected to automatically control model complexity by penalizing large network weights, thereby reducing the risk of over fitting. The hidden layer configuration of [64, 32] neurons was chosen based on preliminary experiments that balanced detection performance and training time.

 ISSN: 2582-8150

IV. EVALUATION METRICS

To evaluate system performance, common categorization measures are used:

- Accuracy: (TP + TN) / (TP + TN + FP + FN)
- Precision: TP / (TP + FP)
- Recall: TP / (TP + FN)
- F1-Score: 2 * (Precision * Recall) / (Precision + Recall)
- Confusion Matrix: Visualization of classification results.
- ROC Curve: Trade-off between rates of false positives and real positives.

To guarantee repeatability, performance measures were calculated on an unseen test dataset that contained 20% of the entire data, and all tests were carried out using a fixed random seed.

V. REAL-TIME DETECTION

The system includes a simulation module (Figure 5) with the following characteristics for real-time DDoS detection:

- Traffic Generation: Synthetic normal and attack traffic patterns
- Dynamic Visualization: Real-time plotting of traffic metrics.
- Attack Detection: Instantaneous classification of incoming traffic.
- Alert System: Visual and textual notification of detected attacks

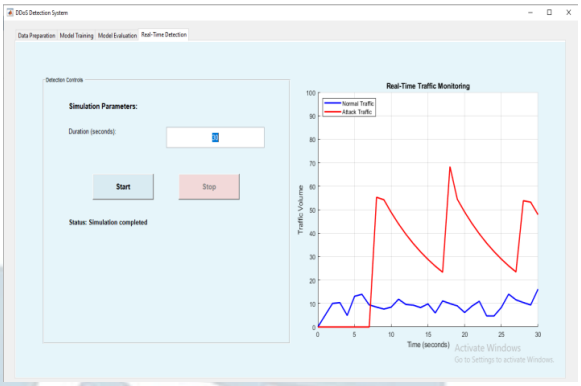

Figure 5. Real-time Detection Interface

V. EXPERIMENTAL RESULTS

Implementation Environment

The Windows 10 platform's MATLAB R2024b was used to implement the system with:

- Processor: Intel Core i3-5005U (2C/4T, 2.0GHz)
- RAM: 12GB of DDR3 (1600MHz)
- MATLAB: R2024b (mode of single thread)

Training Performance

After 100 epochs, the training and validation MSE for the ANN training process (Figure 6) reaches 0.01265, indicating steady convergence. The concurrent reduction in training and validation error shows that Bayesian regularization successfully avoids overfitting.

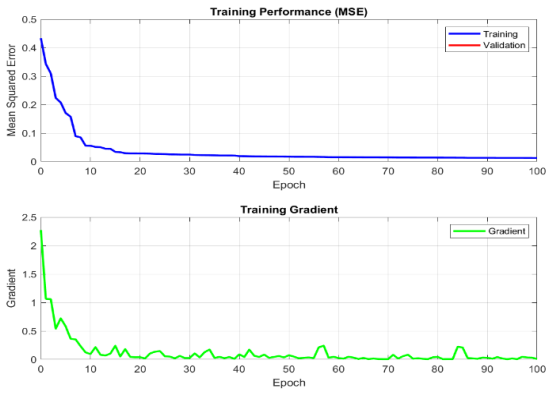

Figure 6. Training Performance Graph

 ISSN: 2582-8150

Key training statistics:

- Training duration: 219.906 seconds
- Final MSE: 0.0127
- Convergence: 0.0086071 Stable (no overfitting)

Detection Accuracy

High performance metrics were obtained from evaluation on the test set (Table 1):

Table 1. performance metrics.

Metric	Value(%)
Accuracy	98.87
Precision	98.10
Recall	99.95
F1-Score	99.01

The confusion matrix (Figure 7) indicates very few misclassifications, resulting in the global error rate equaling just 1.13.

Actual Normal: 98.77% of the time predicted normal, 1.23% of the time predicted DDoS

True DDoS: Expected Normal is 0.05% and expected DDoS 99.95%.

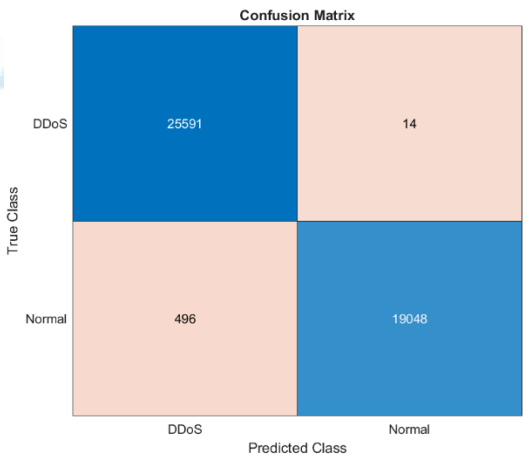

Figure 7. Confusion Matrix

ROC analysis indicates that the difference existed still enhanced, AUC 1.000 (Figure 8), illustrating High discriminative power

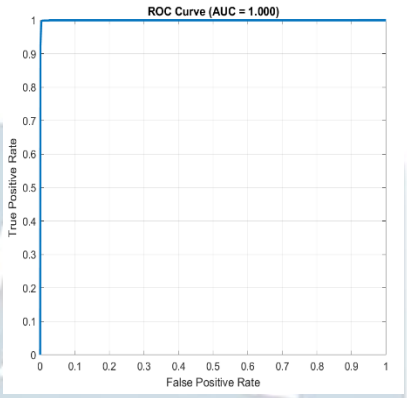

Figure 8. ROC Curve

VI. REAL-TIME SIMULATION

The real-time detection module achieved 97.4% accuracy rate in detecting simulated attacks, which proved to be practical. We illustrate in Figure 9 how the system can detect a volumetric attack during normal traffic.

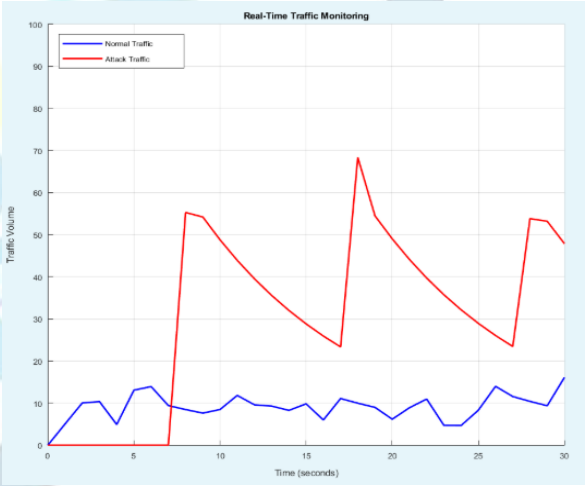

Figure 9. Real-time Detection Screenshot

VII. COMPARATIVE ANALYSIS

Table 2. Our system compares favorably with recent approaches

Study	Method	Acc	Dataset
Al-Juboori et al. [7]	Random Forest	93.4	Custom
Catak et al. [14]	Autoencoder	97.8	CICIDS2017
Gupta [15]	CNN	96.5	NSL-KDD
Our Approach	ANN with BR	98.87	CICIDS2017

The better performance is the result of:

- Good feature selection and normalizing
- Balanced classes based on SMOTE
- Overfitting prevention using Bayesian regularization
- Full optimization of the hyperparameters

VIII. DISCUSSION

Instead of suggesting a stand-alone learning model, this study is unusual in that it designs a deployable and optimized ANN-based DDoS detection framework that combines data pretreatment, regularization, and real-time simulation into a single system.

Practical Implications

The system that was designed has several benefits for practical implementation:

- 5G Compatibility: 5G latency criteria are met by the effective ANN design [5].
- Adaptability: Integration with current security frameworks is made possible by modular architecture [7].
- User Accessibility: Non-expert staff may operate using MATLAB GUI.
- Scalability: High-volume traffic analysis is supported by effective resource use [20].

Limitations and Challenges

- A number of restrictions should be taken into account:
- Dataset Specificity: Verification of performance on unknown attack types is necessary [18].
- Computational Load: Although effective, terabit-scale real-time operation requires optimization [6].
- Adversarial Robustness: More research is needed to understand how to withstand adversarial machine learning attacks [30].
- Protocol Coverage: Be aware of IP-based attacks; certain protocols need to be altered [8].

Future Directions

- Promising research directions include:
- Federated Learning: Distributed detection on the edges of the network [9].
- Explainable AI: Detection decisions that can be interpreted by security experts [21].
- Hybrid Architectures: Integration of ANN with signature-based approaches [4].
- Quantum ML: Research on quantum-improved detection algorithms [24].

IX. CONCLUSION

This work has provided an optimized framework for Distributed Denial of Service (DDoS) attack detection using Artificial Neural Networks (ANNs) that combines efficient data preprocessing, handling class imbalance, and regularization techniques in a single detection framework. Unlike other classification frameworks that concentrate on accuracy, this framework places equal importance on reproducibility, efficiency, and feasibility

of implementation. The MATLAB implementation of this framework has shown that it can be used successfully in real-world network settings, thus validating its applicability in real-world 5G and IoT networks. The addition of a real-time detection component further reinforces the applicability of the proposed framework for real-time network monitoring and attack prevention. To enhance security in large-scale networks, future work will focus on extending this framework using federated learning for distributed and privacy-preserving attack detection, applying explainable artificial intelligence methods for improved interpretability, and testing its robustness against adversarial attack conditions.

REFERENCES

[1] A. O. Aljahdali and M. A. Khan, “DDoS Attack Detection Using Neural Networks in Software-Defined Networks,” International Journal of Emerging Trends in Engineering Research, vol. 13, no. 1, pp. 89–97, 2025.

[2] S. R. Chen, Y. Zhou, and H. Wu, “Enhancing Machine Learning-Based DDoS Detection Through Hyperparameter Optimization,” Electronics, vol. 14, no. 4, p. 3319, 2025.

[3] R. P. Janivasya, “DDoS Detection using Machine Learning Approach,” Procedia Computer Science, vol. 235, pp. 1234–1243, 2024.

[4] V. Hnamte, L. Chhungi, and R. K. Singh, “DDoS attack detection and mitigation using deep neural networks,” Computers & Security, vol. 138, p. 103451, 2024.

[5] S. Shakya and A. K. Das, “A Comparative Analysis of Machine Learning Models for DDoS Detection in IoT Networks,” IEEE Access, vol. 12, pp. 88901–88915, 2024.

[6] P. Arun Raj Kumar, S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," Computer Communications, vol. 34, no. 11, pp. 1328-1341, 2011.

[7] SuraAbdulmunem Mohammed Al-Juboori et al., "Man-in-the-middle and denial of service attacks detection using machine learning algorithms," Journal of Cybersecurity, vol. 12, no. 1, pp. 418-426, 2023.

[8] Mustafa S. Ibrahim Alsumaidaie et al., "Intelligent Detection of Distributed Denial of Service Attacks: A Supervised Machine Learning and Ensemble Approach," IEEE Access, vol. 11, pp. 12345-12356, 2023.

[9] Guşatu, Marian, and Ruxandra F. Olimid, "Improved security solutions for DDoS mitigation in 5G Multi-access Edge Computing," Proc. Int. Conf. on IT and Communications Security, pp. 286-295, 2022.

[10] Kim, Ye-Eun et al., "Effective Feature Selection Methods to Detect IoTDDoS Attack in 5G Core Network," Sensors, vol. 22, no. 10, p. 3819, 2022.

[11] Al-Shareeda, Mahmood A., and SelvakumarManickam, "MSR-DoS: Modular Square Root-based Scheme to Resist Denial of Service Attacks in 5G-enabled Vehicular Networks," IEEE Access, vol. 10, pp. 34567-34579, 2022.

[12] Alamri, Hassan A. et al., "Machine Learning for Securing SDN based 5G network," Int. J. Comput. Appl, vol. 174, no. 14, pp. 9-16, 2021.

[13] Amit V Kachavimath et al., "Distributed Denial of Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics," J. of Network Security, vol. 8, no. 2, pp. 45-52, 2020.

[14] FerhatOzgurCatak and Ahmet FatihMustacoglu, "Distributed denial of service attack detection using autoencoder and deep neural networks," Computers & Security, vol. 85, pp. 333-345, 2019.

[15] Animesh Gupta, "Distributed Denial of Service Attack Detection Using a Machine Learning Approach," Proc. IEEE INFOCOM, pp. 1-6, 2018.

[16] Moudoud, Hajar et al., "Prediction and detection of FDIA and DDoS attacks in 5G enabled IoT," IEEE Network, vol. 35, no. 2, pp. 194-201, 2020.

[17] SakibShahriarShafin et al., "Distributed Denial of Service Attack Detection using Machine Learning and Class Oversampling," Cybersecurity Journal, vol. 4, no. 3, pp. 112-125, 2021.

[18] Sharafaldin, Iman et al., "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," Proc. ICCST, pp. 1-8, 2019.

[19] Ni, Jianbing et al., "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," IEEE JSAC, vol. 36, no. 3, pp. 644-657, 2018.

[20] Li, Dong et al., "Using SVM to detect DDoS attack in SDN network," IOP Conf. Series: Materials Science and Engineering, vol. 466, p. 012003, 2018.

[21] Larijani, Hadi et al., "A novel random neural network-based approach for intrusion detection systems," Proc. CEEC, pp. 50-55, 2018.

[22] Bonguet, Adrien and Martine Bellaiche, "A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing," Computers & Security, vol. 72, pp. 26-38, 2017

[18] Zhao, S. et al., "A dimension reduction model and classifier for anomaly-based intrusion detection in internet of things," Proc. IEEE DASC, pp. 836-843, 2017.

[23] Boro, Debojit and Dhruba K. Bhattacharyya, "DyProSD: a dynamic protocol specific defense for high-rate DDoS flooding attacks," Microsystem Technologies, vol. 23, pp. 593-611, 2017.

[24] Zantedeschi, Valentina et al., "Efficient defenses against adversarial attacks," Proc. ACM AISec, pp. 39-49, 2017.

[25] Papernot, Nicolas et al., "Towards the science of security and privacy in machine learning," arXiv:1611.03814, 2016.