IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 February 2025, accepted 21 March 2025, date of publication 4 April 2025, date of current version 5 May 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3557822

RESEARCH ARTICLE

F-OSFA: A Fog Level Generalizable Solution for Zero-Day DDOS Attacks Detection

MUHAMMAD RASHID MINHAS[1], QAISAR M. SHAFI[2], SHOAB AHMED KHAN[1], TAHIR AHMAD[3], SUBHAN ULLAH[2], ATTAULLAH BURIRO[4], AND MUHAMMAD AZFAR YAQUB[4], (Member, IEEE)

[1]Sir Syed CASE Institute of Technology, Islamabad 44000, Pakistan
[2]FAST-NUCES, Islamabad 44000, Pakistan
[3]Center for Cybersecurity, Bruno Kessler Foundation, Trento, Italy
[4]Faculty of Engineering, Free University of Bozen-Bolzano, 39100 Bolzano, Italy

Corresponding author: Muhammad Azfar Yaqub (myaqub@unibz.it)

ABSTRACT The globalization and digitization of society have caused a surge in network traffic, making reliable online services essential for user trust and system functionality. However, these services face ever-increasing threats, particularly complex and well-developed Distributed Denial of Service (DDoS) attacks. Zero-day DDoS attacks, a type of DDoS attack, are especially challenging because their new and unseen nature and lack of training data render traditional Intrusion Detection and Prevention Systems (IDPS) ineffective. To tackle this, we propose the Fog-based One Solution For All (F-OSFA) system - a model with three specialized components. The first component uses a hybrid machine learning and deep learning framework that combines convolutional neural networks (CNNs) and decision trees to detect traditional DDoS attacks. The second component employs a few-shot learning module with a contractive autoencoder for zero-day attack detection. The third component is a signature-based resource usage analyzer to counter attacks mimicking normal traffic. We demonstrate the efficacy of F-OSFA on publicly available datasets and prove the scheme is generalizable and effective. F-OSFA achieves an accuracy of 99.72% on CICDDoS2019 and 99.96% on CICIDS2017. In addition, it demonstrates its efficacy in the zero-day scenario as well by achieving a 96.77% on CICDDoS2019 and 95.98% on CICIDS2017. These evaluations testify to F-OSFA as a reliable and versatile solution against ever-evolving DDoS threats.

INDEX TERMS Distributed denial of service, convolutional neural network, intrusion detection and prevention system, zero-day detection.

I. INTRODUCTION

The Internet has transformed human life, enabling advancements in areas ranging from routine tasks to complex business operations. The emergence of cloud computing has further established the Internet as the backbone of the digital industry, influencing sectors such as healthcare, finance, entertainment, smart cities, and governance [1]. Similarly, the Internet of Things (IoT), introduced in 1999, has revolutionized data collection and communication for real-time decision-making in applications such as healthcare, manufacturing, transportation, and energy [2], [3]. The rapid adoption of IoT has led to unprecedented growth. This surge in connected devices and online platforms has significantly increased network traffic, making availability and security more critical than ever before. However, Distributed Denial of Service (DDoS) attacks, particularly zero-day variants, pose severe threats to network availability [2]. These attacks leverage large botnets to overwhelm the resources of a victim, causing them to be unable to serve legitimate users [4]. Recent high-profile DDoS incidents, including attacks on Google and AWS with peak volumes exceeding 2 Tbps, highlight the growing scale of this challenge [5], [6].

Intrusion Detection and Prevention Systems (IDPS) have been developed to address these security challenges using various techniques. IDPS are broadly categorized into two

The associate editor coordinating the review of this manuscript and approving it for publication was Vicente Alarcon-Aquino.

types [7], [8]: Anomaly-Based IDPS [9] and Signature-Based IDPS [7]. Existing defensive mechanisms typically focus on specific aspects of the broader security challenge, limiting their ability to generalize effectively. Anomaly-based IDPS are trained and tested on known datasets, effectively detecting attacks with familiar patterns. However, they often fail to perform adequately against variants of known attacks and unknown or zero-day DDoS attacks [10]. Adversaries often design attacks with behaviours that remain below the anomaly detection thresholds, further complicating their identification. Signature-based IDPS, on the other hand, relies on predefined attack signatures to identify malicious activities. Although effective against known attack patterns, they face significant challenges in detecting novel or zero-day attacks due to the difficulty of collecting comprehensive datasets that encompass all possible DDoS attack signatures. Consequently, these systems are limited in addressing the evolving nature of network threats.

Traditional intrusion detection and prevention systems (IDPS) fail to address these evolving threats. Anomaly-based IDPS perform well with known attack patterns but struggle with zero-day attacks. At the same time, signature-based systems are limited by the difficulty of obtaining comprehensive datasets for new attack signatures [10]. Moreover, the limitations of cloud-based solutions, such as latency in real-time detection, and the affordability-driven simplicity of IoT devices such as low intelligence, along with the complexity of network traffic which can be observed from the latest datasets of DDoS based on more than 80 features in both CICDDoS2019 and CICIDS2017 representing high dimensional feature space as justified using tSNE visualization as in Figure 3 and Andrew Curve as shown in Figure 4 exacerbate these challenges [11]. Fog level is basically proposed to address shortcomings of the cloud concerning security challenges with advantages of low latency, taking intelligence nearer to end devices, and distributed computing.

Due to complex nonlinear network traffic and ever-evolving advancements in the signature of threat and real-world scenarios, the threat faced in multi-dimensional space requires a multi-prong solution based on deep learning techniques where each prong is specially designed to counter specific categories of attacks. To address these gaps, we propose the Fog-based One Solution For All (F-OSFA), a multi-pronged defense system designed to counter complex and diverse DDoS threats. By introducing a fog layer between IoT devices and the cloud, F-OSFA reduces latency while enhancing security [12] and brings intelligence nearer to the end devices. The proposed system comprises three prongs: a hybrid deep learning model for traditional DDoS detection, a Zero-Shot Learning (ZSL) module based on semi-supervised Contractive Autoencoders for Zero-day attacks, and a signature-based resource usage analyzer for detecting mimicked traffic patterns. This architecture ensures comprehensive and real-time defense against the multidimensional challenges of modern network traffic.

The main contributions of the paper are the following:

- **In-depth study of network traffic**: In-depth study of network traffic flow regarding all types of data that can be available in it.
- **Comprehensive Defense System for DDoS Attacks**: The paper proposes the Fog-based One Solution For All (F-OSFA), a multi-pronged defense system that addresses a wide spectrum of DDoS attacks, including traditional, zero-day, and mimicked traffic attacks.
- **Zero-Shot Learning (ZSL) Approach**: The introduction of a semi-supervised Zero-Shot Learning module based on Contractive Autoencoders (CAE) effectively detects Zero-day DDoS attacks. This approach minimizes dependency on attack data by accurately classifying previously unseen attack patterns.
- **Hybrid Deep Learning Framework**: Using a hybrid model combining Convolutional Neural Networks (CNN) and Decision Trees enhances complex, high-dimensional network traffic classification, offering robust detection of traditional DDoS attacks.
- **Generalizability and Real-World Validation**: The proposed F-OSFA system is validated on CICIDS2017 and CICDDoS2019 datasets, demonstrating high accuracy not only against DDoS attacks but also other types of network threats. Its adaptability ensures effectiveness across diverse real-world scenarios.
- **Evaluation of Zero Day DDoS Attack Scenario**: The proposed F-OSFA system is also validated on zero day DDoS Attack scenario from CICIDS2017 and CICDDoS2019 datasets, demonstrating high accuracy not only against known DDoS attacks but also in zero day DDoS Attack scenario.

The rest of the paper is organized as follows: Section II provides the necessary background information to facilitate a better understanding of the underlying technology. Section III reviews relevant studies published over the years, highlighting the research gaps addressed in this work. Section IV details the proposed methodology employed to address the detection problem. Section V presents the experimental analysis, while the results and discussions are provided in Section VI. Finally, Section VII concludes the paper and outlines potential directions for future work.

II. BACKGROUND

A. FOG COMPUTING

Fog computing is a decentralized computing paradigm that brings computation and storage closer to the network edge. Unlike the centralized cloud, fog computing operates near edge devices, providing cloud-like services such as computation, storage, and data processing directly at the edge [12], [13]. Positioned at the network's geographical boundaries, fog computing minimizes latency, enabling real-time data analysis, improved quality-of-service, and efficient management of highly distributed IoT networks [14]. The architecture typically comprises three layers: the cloud

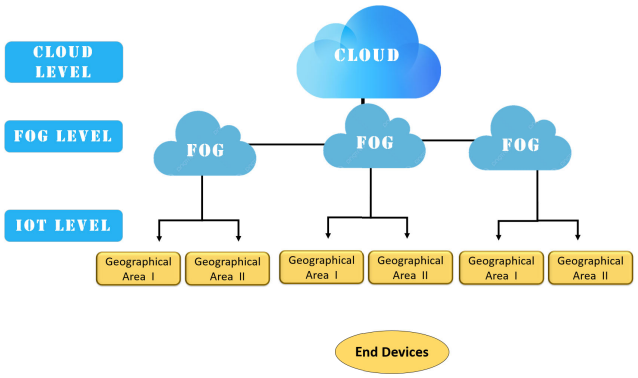


FIGURE 1. Fog infrastructure.

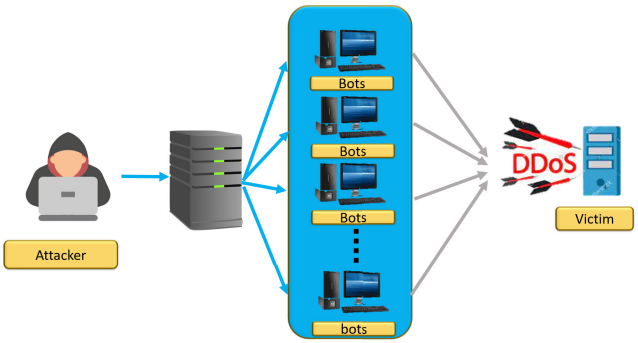


FIGURE 2. DDoS attack based On Botnets.

(highest), fog (intermediate), and IoT devices (lowest), as shown in Figure 1. Fog computing addresses key cloud limitations like latency in real-time IoT applications, making it crucial for fields such as autonomous driving, smart cities, industrial IoT, agriculture, and healthcare [11].

B. DISTRIBUTED DENIAL OF SERVICE (DDOS)

A Distributed Denial-of-Service (DDoS) attack involves an attacker exploiting a large network of compromised devices (botnets) to overwhelm a target's network with excessive traffic. This disrupts service availability by consuming the victim's resources, preventing legitimate users from accessing services [2]. DDoS attacks fall into three primary categories: Traditional DDoS, Unknown/Zero-day DDoS (characterized by novel signatures) [4], and Mimicking Normal Traffic attacks. Traditional attacks are further classified into protocol-based, application-layer, and volumetric attacks. Zero-day DDoS attacks, being unpredictable, can span any category, making detection and mitigation particularly challenging. Figure 2 illustrates the basic concept of a botnet-driven DDoS attack.

C. INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

Intrusion Detection and Prevention Systems (IDPS) monitor network traffic to detect and respond to malicious activity [7]. IDPS is categorized into two main types: anomaly-based and signature-based systems [8].

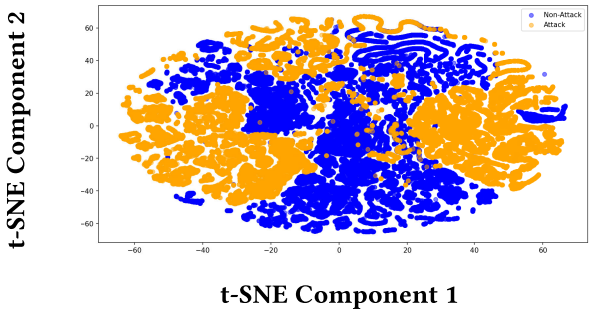


FIGURE 3. t-SNE visualization for CIC-IDS2017.

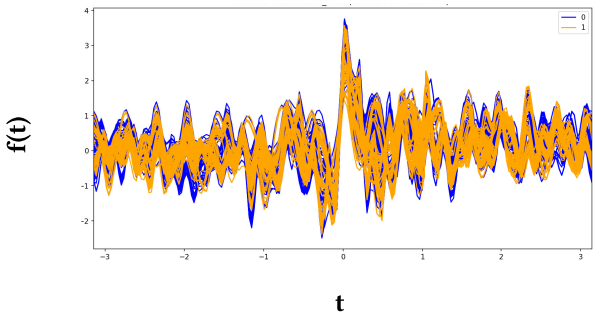


FIGURE 4. Andrews curve of CICIDS2017.

Anomaly-based IDPS establishes a baseline of normal network behaviour and identifies deviations as potential threats [7]. It excels at detecting unknown attacks but struggles with fine-grained threshold tuning and variants designed to bypass detection. Signature-based IDPS, in contrast, detects threats by comparing traffic against a database of predefined attack signatures [15]. While effective against known attacks, it fails to identify new or Zero-day threats [7].

Existing defensive mechanisms often address specific aspects of the DDoS problem but lack generalizability for real-world scenarios where threats are multi-dimensional. Effective mitigation requires a holistic approach capable of handling normal traffic, traditional attacks, mimicking traffic, and Zero-day attacks simultaneously. However, current machine learning (ML) and deep learning (DL) classifiers perform suboptimally against these diverse challenges, particularly Zero-day attacks, due to their dependence on known patterns [10].

Understanding the complexity of network traffic is essential for developing generalizable solutions. Real-world datasets like CICDDoS2019 and CICIDS2017 highlight this complexity, featuring high-dimensional data with over 80 attributes. Figures 3 and 4 illustrate the non-linearity of network data using t-SNE and Andrews Curve visualizations, revealing significant overlap between attack and normal instances, complicating traditional classification methods.

Deep learning (DL) techniques have shown remarkable performance in addressing such complexities due to their ability to extract intricate features and handle high-dimensional, non-linear data [16]. Unlike traditional approaches, DL-based architectures are well-suited for diverse traffic patterns, making them effective for real-world

scenarios. Leveraging these strengths, a multi-pronged DL-based system offers the best prospects for tackling the evolving landscape of DDoS threats [17], [18].

III. LITERATURE REVIEW

This section highlights significant research contributions in the field of information security, focusing on DDoS attack mitigation in IoT and fog computing environments.

A. DDOS ATTACKS

Sharafaldin et al. [19] present a taxonomy of DDoS attacks and defense mechanisms, providing a detailed analysis of various methods. Vishwakarma and Jain [20] explore IoT network's growth potential and services, briefly discussing botnet-based DDoS attacks, attack taxonomies, and defense mechanisms, including ML and DL approaches.

B. AUTOENCODER FOR ZSL MODULE

In [10], a contractive autoencoder-based IDPS is proposed for attack detection using datasets such as CICIDS2017, NSL-KDD, and CIC-DDoS2019. The model achieves 93.41%-97.58% accuracy on CICDDoS2019, 96.08% on NSL-KD, and 92.45% on CICIDS2017. Tang et al. [21] propose an unsupervised LSTM-based encoder-decoder framework evaluated on 1.4 billion web requests, using reconstruction errors for attack detection. Zhang et al. [22] introduce a ZSL architecture using sparse autoencoders, achieving 88.3% accuracy on NSL-KDD. Zhai et al. [23] provide a survey on various autoencoder types, including convolutional, sparse, contractive, and adversarial AE. Hindy et al. [18] propose ANN-based autoencoders with zero-day detection accuracies of 75%-98% for CICIDS2017 and 89%-99% for NSL-KDD. Tan et al. [24] offer a comprehensive survey on ZSL methods and applications.

C. AUTOENCODER FOR DIMENSION REDUCTION AND OUTLIER DETECTION

Singh and Jang [25] utilize Multi-Scale CNN for spatial features and LSTM-based AE for temporal features, integrating Isolation Forest for error correction. Wei et al. [26] combine AE-MLP, achieving F1-scores above 98%. Fardusy et al. [27] propose AE-SVM models with 99.57% accuracy on CICDDoS2019. Elsayed et al. [16] develop LSTM-based autoencoders with OCSVM, using benign traffic for training. Min et al. [28] introduce Memory-Augmented Deep AE, achieving a 95% F1-score on NSL-KDD. Wang et al. [13] use stacked contractive autoencoders (SCAE) with SVM for binary classification, achieving 88.73% accuracy on NSL-KDD.

D. IDPS USING ML

Elmasri et al. [29] propose KNN, enhanced KNN, and LOF, with LOF achieving 90.5% average accuracy. Nazarudeen and Sundar [30] use Extra Tree classifiers for feature extraction, applying Decision Trees, XGBoost, and Random Forest, with DT and RF achieving 99% accuracy on CICDDoS2019. Sharma and Babar [31] analyze ML models, including KNN, Naive Bayes, DT, and RF, demonstrating strong detection capabilities.

E. IDPS USING DL

F. FOG LEVEL

Shafi et al. [32] propose an SDN-based IDPS for fog level, integrating IDPS Coordinator, Resource Manager, SDN Fabric Manager, and Feature Selector, using E3CL with RNN, MLP, and Alternate Decision Trees. Minhaz et al. [33], and Priyadarshini and Rabindea [34] propose fog-level architectures to address IoT security challenges, highlighting three-layer models consisting of IoT, Fog, and Cloud levels.

Our approach advances the state-of-the-art by addressing the multi-dimensional threat of DDoS attacks and the ever-evolving threat of zero-day DDoS attacks by proposing a multi-prong defense system at the fog level. This addresses the latency limitation of cloud architecture and the intelligence limitation of IoTs by bringing intelligence nearer to end devices without adding it to end devices and enabling distributed computing. Each prong of the proposed system is designed to mitigate a specific attack category. This hybrid design, coupled with a voting mechanism, ensures high accuracy and robust detection of known and zero-day DDoS attacks, outperforming prior studies in intrusion detection for IoT-based networks. It has achieved state-of-the-art accuracy of 99.72% on CICDDoS2019, 99.96% on the DDoS dataset of CICIDS2017, and 99.65% on the complete dataset of CICIDS2017. In addition, it demonstrates its efficacy in the zero-day scenario, achieving 96. 77% on CICDDoS2019 and 95.98% on CICIDS2017, as shown in table 1. The research transcends traditional methodological boundaries by rigorously simulating zero-day attack scenarios, offering a sophisticated and generalizable framework for detecting previously uncharacterized network intrusion strategies.

IV. METHODOLOGY

Real-world DDoS threats require a generalizable solution effective against all attack categories, including Zero-day DDoS. We propose F-OSFA, a multi-prong defense mechanism comprising three modules tailored to a specific attack category (Figure 5). Prong 1 employs a Hybrid DL/ML classifier for detecting known attacks with high accuracy. Prong 2 integrates a CAE-based Zero-Shot Learning (ZSL) module to detect unknown and Zero-day DDoS attacks. Prong 3 implements a signature-based resource usage analyzer to identify mimicked traffic patterns.

Incoming traffic undergoes initial filtering through a firewall, followed by preprocessing and parallel analysis by all three prongs. A decision-making mechanism aggregates results, prioritizing maximum detection accuracy. Malicious traffic is blocked, and its IP addresses are dynamically blacklisted to prevent future attacks. This architecture ensures

TABLE 1. Comparison of proposed approach with state of the art.

Reference	Approach	Dataset	Key Features
Sharafaldin et al. [19]	- Taxonomy of DDoS attacks and defense mechanisms		- Survey Analysis of various DDoS attack methods and defenses
Aktar and Nur [10]	- Contractive autoencoder-based IDPS	- CICIDS2017 - NSL-KDD - CIC-DDoS2019	- Accuracy: 93.41%-97.58% (CICDDoS2019) - 96.08% (NSL-KDD), 92.45% (CICIDS2017) - Semi Supervised Approach - Do not cater for mimic normal traffic DDoS Attacks
Tang et al. [21]	- Unsupervised LSTM based encoder-decoder framework	- 1.4 billion web requests	- ZSL Approach - Unsupervised LSTM based encoder-decoder framework to detect attacks - Do not cater for mimic normal traffic DDoS Attacks
Zhang et al. [22]	- ZSL architecture using sparse autoencoders	- NSL-KDD	- Accuracy: 88.3% - ZSL Approach - Do not cater for mimic normal traffic DDoS Attacks
Zhai et al. [23]	- Survey on various autoencoder types		- Comprehensive coverage of AE variants including sparse, contractive, and adversarial AEs
Hindy et al. [18]	- ANN-based autoencoders for zero-day detection	- CICIDS2017 - NSL-KDD	- Accuracy: 75%-98% (CICIDS2017) - 89%-99% (NSL-KDD) - ZSL Approach and do not cater for mimic normal traffic DDoS Attacks
Singh and Jang [25]	- MS CNN AE for feature extraction - LSTM AE for capturing temporal dependencies and Isolation Forests for error correction.		- Combines spatial-temporal feature learning - Integrates Isolation Forest for improved outlier detection - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Wei et al. [26]	- Dimensionality reduction using AE + MLP for classification		- Achieves F1-scores > 98% for DDoS detection - Dimensionality reduction using AE, MLP for classification - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Fardusy et al. [27]	- AE-SVM model	- CICDDoS2019	- Accuracy: 99.57% - Dimensionality reduction using AE - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Elsayed et al. [16]	- LSTM-based autoencoders with OCSVM	- Trained on benign traffic	- Uses benign traffic for training - Detects anomalies via reconstruction errors - Do not cater for mimic normal traffic DDoS Attacks
Min et al. [28]	- Memory-Augmented Deep AE	- NSL-KDD	- F1-score: 95% - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Wang et al. [13]	- Stacked contractive autoencoders with SVM	- NSL-KDD	- Accuracy: 88.73% - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Elmasri et al. [29]	- KNN, Enhanced KNN, and Local Outlier Factor (LOF)	- CICIDS2017	- LOF achieves 90.5% average accuracy - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Nazarudeen et al. [30]	- Extra Tree Classifiers for feature selection + DT, XGBoost, RF	- CICDDoS2019	- DT and RF achieve 99% accuracy - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Sharma and Babar [31]	- Comparative analysis of ML algorithms (KNN, NB, DT, RF)		- Evaluates ML models for IoT-based DDoS detection - highlights strong performance of DT and RF
Mohammadpour et al. [35]	- Survey of CNN-based intrusion detection systems (IDPS)		- Survey Paper - Reviews CNN architectures for network intrusion detection
Jinsi and Deepa [36]	- Comparison of DNN, CNN, LSTM	- CICIDS2017	- CNN achieves 98.61% - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Boonchai et al. [37]	- DNN and convolutional AE	- CICDDoS2019	- Classifies DDoS attacks with 81.2%–85.1% accuracy - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Yuan et al. [38]	- **DeepDefense**: Hybrid CNN, LSTM, and GRU architecture		- Combines CNN for spatial features and LSTM / GRU for temporal analysis - Do not cater for zero day DDoS Attacks and mimic normal traffic DDoS Attacks
Minhaz et al. [33]	- Fog-based DDoS detection with DL + Random Forest feature selection		- Use of fog layer for IoT security
Priyadarshini & Rabindea [34]	- Deep learning-based fog framework		- Use of fog layer for IoT security
Proposed F-OSFA	- Fog-based One Solution For All (F-OSFA) system a model with three specialized components; - Hybrid ML/DL framework combining CNNs and decision treea - Few-shot learning module with a semi supervised contractive AE for zero-day attack detection - Signature-based resource usage analyzer to counter mimic normal traffic	- CICDDoS2019 - CICIDS2017	- Highly generalizable approach for today's complex network traffic - Accuracy: 99.72% on CICDDoS2019 - Accuracy: 99.96% on CICIDS2017 - Cater for zero day DDoS Attacks - Cater for mimic normal traffic DDoS Attacks

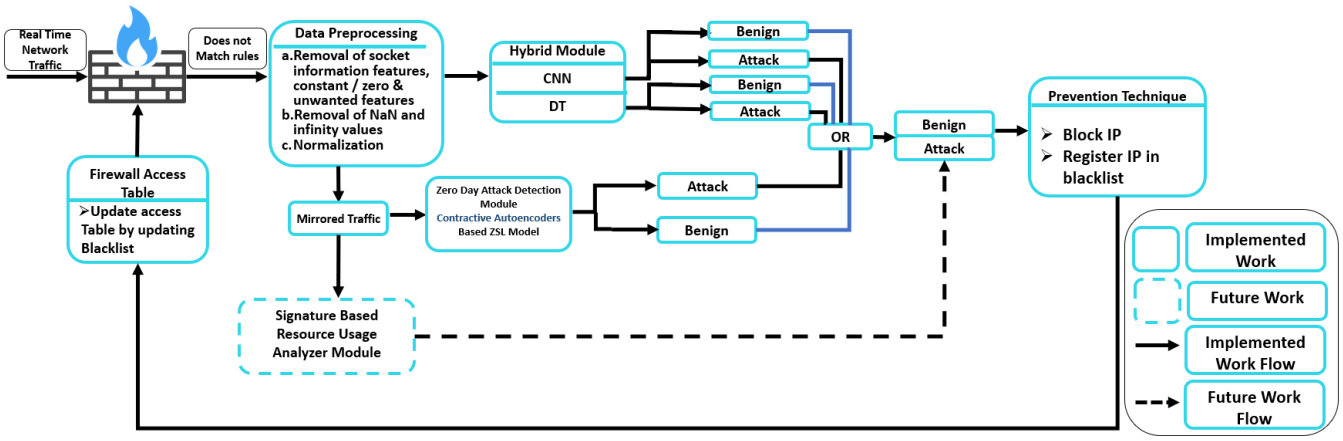


FIGURE 5. Architecture of proposed multi prong defense mechanism F-OSFA.

robust, real-time DDoS mitigation across diverse threat scenarios.

A. PRONG 1: HYBRID MODULE

Prong 1 is designed to detect known attacks and traditional categories of DDoS attacks with high accuracy. Deep learning (DL) has emerged as a preferred technique for handling high-dimensional, nonlinear, and complex network traffic data [8], [10], [17], [18], [32], [38]. Models like CNN [25], [35], [37], [39], RNN, and various autoencoder (AE) types, including sparse and contractive AEs, have been extensively studied. These models autonomously extract meaningful features, eliminating the need for manual feature engineering. Given the high dimensionality and nonlinearity of DDoS attack data, DL could offer superior efficiency.

In this prong, we employ CNN and Decision Trees (DT) based on their proven performance, as supported by experimental results and relevant research [35], [37], [39]. CNN has demonstrated remarkable success in complex tasks, from data classification to enabling autonomous vehicles, and has been widely utilized in intrusion detection [25], [35], [37], [39]. DTs are particularly effective in known attack scenarios, as highlighted in Table 7.

B. OUR MODEL

This section introduces the proposed CNN architecture in the hybrid prong for network traffic classification. The CNN comprises two convolutional layers: the first with 64 neurons, a 3×3 kernel, and ReLU activation, and the second with 32 neurons, a 2×2 kernel, and ReLU activation. A flattened layer converts the output into a one-dimensional array, followed by a Dense layer with 128 neurons and ReLU activation for learning complex patterns. The final Dense layer has two neurons with a softmax activation function. The model uses a batch size of 32 and runs for 5 epochs.

C. DECISION TREES

Decision Trees (DT) are supervised machine learning algorithms that are highly versatile for classification and regression problems. They utilize a tree-like structure, where binary decisions are made at each node, and each leaf node represents an outcome [30], [31]. This hierarchical structure captures complex decision boundaries effectively. The algorithm processes data from the root through binary decisions at each node based on specified thresholds, directing the flow to the appropriate branches.

D. PRONG 2: ZSL MODULE

Prong 2 is designed to address zero-day DDoS attacks specifically while also contributing to detecting other DDoS categories. Traditional ML models are limited to recognizing classes encountered during training. However, real-world scenarios often include zero-day DDoS attacks for which labelled data is unavailable. Zero-shot learning (ZSL) overcomes this limitation by reducing dependency on attack data and training instead of easily accessible benign traffic.

E. AUTOENCODERS

The ZSL module in the proposed architecture utilizes an autoencoder (AE) in a semi-supervised learning setup. The AE consists of an encoding stage that compresses input data into a low-dimensional representation and a decoding stage that reconstructs the input from this compressed code (Figure 6). Contractive AEs (CAE) are used in this module due to their superior performance (Table 7).

F. CONTRACTIVE AUTOENCODER

Unlike basic autoencoders, CAEs extract valuable features while ensuring insensitivity to small variations in input data [10]. This is achieved by adding a penalty term derived from the Frobenius norm of the Jacobian matrix of the encoded features to the objective function. The loss function is defined as follows:

$$|J_f(x)|F^2 = \sum i, j \left(\frac{\partial h_j(x)}{\partial x_i} \right)^2 \quad (1)$$

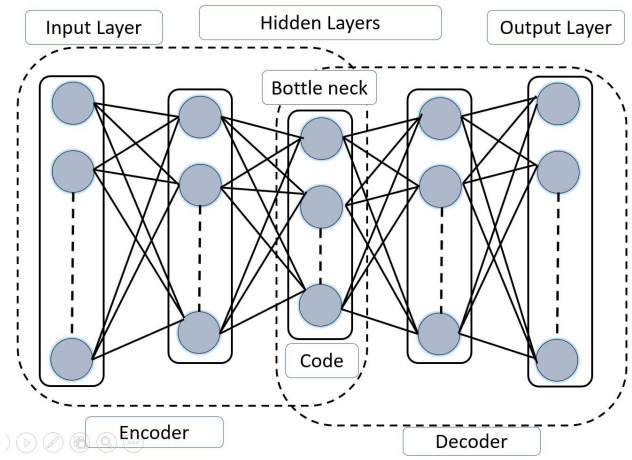


FIGURE 6. Proposed contractive autoencoder.

The CAE's objective function with the regularization term is:

$$J_{\text{CAE}}(\theta) = \sum_{x \in D_x} \left[L(x, g(f(x))) + \lambda |J_f(x)|_F^2 \right] \tag{2}$$

1) OUR MODEL

The ZSL module incorporates a CAE that learns robust input representations and is resilient to minor variations in benign traffic. Trained on benign instances, the CAE reconstructs normal traffic with minimal error but yields higher reconstruction errors for anomalous data. The model comprises two encoder and decoder layers (Figure 6). The encoder reduces dimensions to 32 and 16, while the decoder restores the original dimensions. ReLU is used in hidden layers, and sigmoid is used in the decoder's final layer. The contractive penalty term ensures generalization, making it highly effective for zero-day attack detection.

2) OPTIMAL THRESHOLD CALCULATION

Optimal threshold selection is critical for the ZSL module. Algorithm 1 outlines the procedure for determining the threshold that maximizes detection accuracy. The CAE, trained exclusively on benign data, uses reconstruction error to differentiate between benign and attack instances. A sample is classified as benign if its reconstruction error is below the threshold; otherwise, it is identified as malicious.

The CAE's reconstruction capability efficiently handles benign traffic while producing high reconstruction errors for attack instances. This differentiation allows accurate classification based on reconstruction error thresholds. The working principle of the ZSL module is illustrated in Figure 7. When an input instance is provided to the contractive AE, the encoder generates a code for the respective input, which is then fed to the decoder. The decoder reconstructs the feature sequence from the code of the respective input. The original and reconstructed instances are compared, and if the reconstruction error is within the selected threshold, the input is classified as a normal instance; otherwise, it is classified as an attack instance, as shown in Figure 7.

Algorithm 1 Optimal Threshold Calculation for ZSL Module

Input: Training Data X_{train}
Train ZSL module on X_{train}
$min\_RE = \min(\text{train\_loss})$, $max\_RE = \max(\text{train\_loss})$
$threshold = max\_RE$, $best\_threshold = threshold$
while $threshold > min\_RE$ **do**
    Compute accuracy for current *threshold*
    if accuracy > best_accuracy **then**
        $best\_accuracy \leftarrow$ accuracy, $best\_threshold \leftarrow threshold$
    end if
    $threshold \leftarrow threshold - 0.01$
end while
Return *best_threshold*

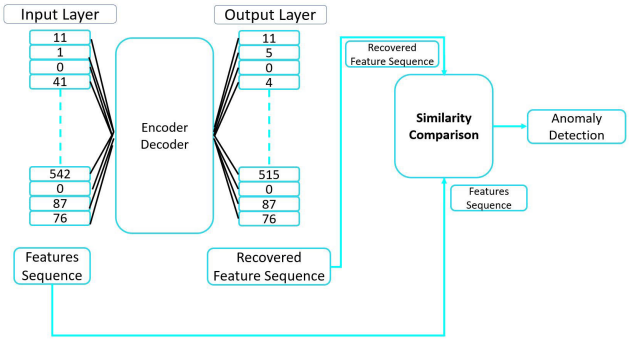


FIGURE 7. Working principle of contractive AE-based ZSL.

TABLE 2. Total instances vs. Used instances in CICDDoS2019.

CICDDoS2019	Total	Benign	Malicious
Training Day	50,063,112	56,863	50,006,249
Testing Day	20,364,525	56,965	20,307,560
Total	70,427,637	113,828	70,313,809
Used	**6,650,000**	113,828 (100%)	6,536,172 (11%)

V. EXPERIMENTAL ANALYSIS

This section comprehensively overviews the experimental procedures, including datasets, preprocessing techniques, evaluation metrics, experimental setup, and results.

A. DATASET

We selected two prominent datasets, CICIDS2017 and CICDDoS2019, widely recognized for their relevance in DoS/DDoS attack detection, to evaluate the proposed architecture.

The CICDDoS2019 dataset [19] is a widely utilized benchmark for DDoS attack detection and classification. This dataset spans two days, capturing attacks from the Reflection and Exploitation categories. The training set includes 12 attack types, while the testing set contains 7 attack types. Instances of all DDoS attacks are taken for evaluation, where Table 2 summarizes instances where each sample contains over 80 features.

The CICIDS2017 dataset [29], developed by the Canadian Institute for Cybersecurity, encompasses many modern network attacks, including DoS/DDoS attacks.

TABLE 3. Constant/Zero value features in CICIDS2017 and CICDDoS2019.

Feature No.	CICIDS2017	CICDDoS2019
1	Bwd PSH Flags	Bwd PSH Flags
2	Bwd URG Flags	Bwd URG Flags
3	Fwd Avg Bytes / Bulk	Fwd Packet / Bulk Avg
4	Fwd Avg Bulk Rate	Bwd Bytes / Bulk Avg
5	Bed Avg Packets / Bulks	Bwd Bulk Rate Avg
6	Fwd URG Flags	Fwd URG Flags
7	CWE Flags Count	Fwd Bytes / Bulk Avg
8	Fwd Avg Packets / Bulk	Fwd Bulk Rate Avg
9	Bwd Avg Bytes / Bulk	Bwd Packet / Bulk Avg
10	Bwd Avg Bulk Rate	–

B. PREPROCESSING

Effective preprocessing is essential for preparing data to achieve optimal performance. The following steps were applied:

- Socket-related features such as Source IP, Destination IP, Source Port, Destination Port, and Protocol were removed to avoid overfitting and ensure network generalizability.
- Non-contributory features, including "Flow ID," "Timestamp," "Flow Bytes," "Flow Packets," and "SimilarHTTP," were excluded.
- Features with constant or zero values were eliminated to reduce the dimensionality of the data. Examples of such features are listed in Table 3.
- Instances with NaN or infinity values were discarded.
- Class labels were converted to numeric values: anomalous instances were labelled as 1, and normal instances were labelled as 0.
- Min-Max normalization was applied to numeric features to scale their values to a range of [0, 1], mitigating the impact of differing feature scales.

To address the imbalance between benign and malicious packets in CICDDoS2019, we randomly sampled 6.5 million attack packets and all benign packets. The datasets were divided into multiple batches to simulate real-world scenarios by transforming known attacks into unknown/zero-day attacks, as shown in Tables 4 and 5. To further increase the dataset's difficulty level, CICDDoS2019 was divided into 15 batches, as shown in Table 4, and CICIDS2017 was divided into 8 batches, as shown in Table 5. This transformation aims to convert known attacks into unknown/zero-day attacks, enabling the proposed architecture to simulate real-world network flow scenarios.

C. EVALUATION METRICS

The performance of the proposed architecture was evaluated using the following metrics:

- **Accuracy:** Ratio of correctly predicted instances to total predictions.
- **Precision:** Ratio of true positive predictions to total positive predictions.
- **Recall:** Ratio of true positive predictions to actual positive instances.
- **F1-Score:** Harmonic mean of precision and recall.
- **Confusion Matrix:** Breakdown of true positives, false positives, true negatives, and false negatives as shown in Table 6.

TABLE 4. 15 x batches of CICDDoS2019.

Batch	Training Attacks	Testing Attacks	Zero-day Attacks
1	4 x Attacks data (not available in testing day)	All testing day attacks	All unknown
2	Batch 1 + NetBIOS,	Same	6 x unknown
3	Batch 2 + 'MSSQL	Same	5 x unknown
4	Batch 3 + NetBIOS	Same	4 x unknown
5	Batch 4 + Syn	Same	3 x unknown
6	Batch 5 + LDAP	Same	2 x unknown
7	Batch 6 + UDPLag	Same	Whole Dataset
8	Batch 7	Same	All known
9	Syn	Same	All Attacks
10	LDAP	LDAP	Single Attack
11	LDAP Lag	LDAP Lag	Single Attack
12	UDAP	UDAP	Single Attack
13	Syn	Syn	Single Attack
14	Netbios	Netbios	Single Attack
15	MSSQL	MSSQL	Single Attack

TABLE 5. 8 x batches of CICIDS2017.

Batch	Training Attacks	Testing Attacks	Zero-day Attacks
1	DOS / DDoS dataset	DOS / DDoS dataset	Known Attack
2	Whole Dataset	Whole Dataset	Known Attack
3	7 Attacks	6 x Attacks	2 x unknown
4	4 attacks	Other 4 attacks	All unknown
5	4 attacks	Other 4 attacks	All unknown
6	4 attacks	Other 4 attacks	All unknown
7	4 attacks	Other 4 attacks	All unknown
8	7 attacks	8 attacks	1 x unknown

TABLE 6. Confusion matrix.

TN	**FP**
FN	**TP**

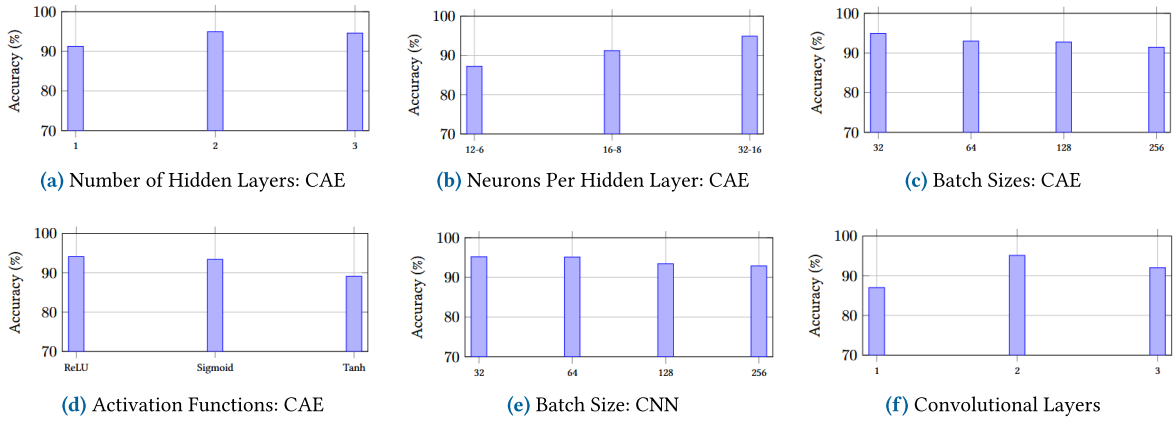
- **True Negative (TN):** Correctly classified benign traffic.
- **False Positive (FP):** Benign traffic incorrectly classified as anomalous.
- **False Negative (FN):** Malicious traffic incorrectly classified as benign.
- **True Positive (TP):** Correctly classified malicious traffic.

D. EXPERIMENTAL SETUP

The experiments were conducted in a PyCharm environment using Python 3.7. The hardware platform was an Acer S5-371 Core i7 6th generation laptop. Keras was used to implement deep learning models. The ZSL module was trained on benign samples, while the hybrid module used normal and attack samples. Various ML and DL models were tested on CICDDoS2019, with results summarized in Table 7. CNN demonstrated superior performance, achieving accuracies of 95% for the full dataset and 91% for zero-day scenarios. CAE outperformed other autoencoders in detecting maximum attack instances.

E. HYPERPARAMETERS OF ALL MODELS

This section discusses the optimal hyperparameter tuning for the algorithms used in the proposed architecture. The Contractive Autoencoder (CAE) was configured for the ZSL module with Contractive Loss as the cost function, using the



(a) Number of Hidden Layers: CAE (b) Neurons Per Hidden Layer: CAE (c) Batch Sizes: CAE

(d) Activation Functions: CAE (e) Batch Size: CNN (f) Convolutional Layers

FIGURE 8. Parameter optimization of AE and CNN.

TABLE 7. Performance comparison of different classifiers on CICDDoS2019.

No.	Model	Accuracy	Zero-Day Accuracy
1	SVM	89.53	74.00
2	RF	90.73	79.01
3	LR	92.12	76.22
4	KNN	89.00	81.00
5	NB	91.00	77.00
6	DT	92.61	84.27
7	ANN	91.14	83.14
8	MLP	92.15	88.11
9	CNN	95.19	90.97
10	RNN	92.38	87.21
11	Basic AE	87.11	81.68
12	CAE	94.89	93.06
13	Sparse AE	84.56	84.76

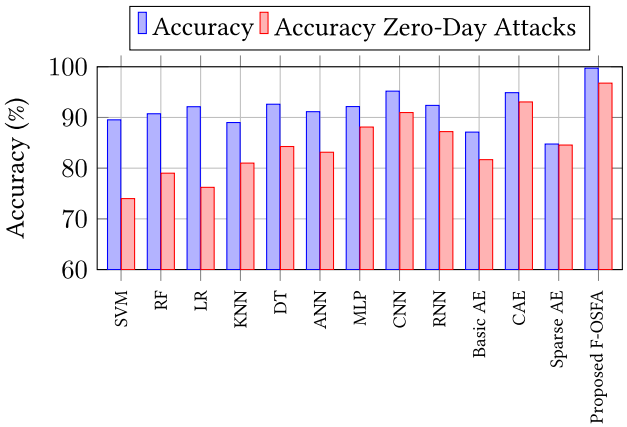


FIGURE 9. Performance comparison of models on zero-day attacks and overall accuracy for CICDDoS2019.

TABLE 8. Proposed F-OSFA against Dos / DDoS (CICIDS2017).

Model	Accuracy	Remarks
Proposed OSFA	99.96	DOS / DDoS dataset of *CICIDS2017*

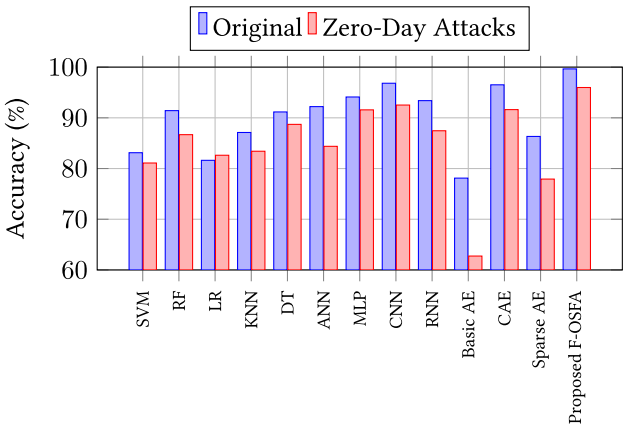


FIGURE 10. Performance comparison of models on zero-day attacks and overall accuracy for CICIDS2017.

Adam optimizer and a batch size of 32. The hidden layers employed ReLU as the activation function, while the output layer used a sigmoid activation function. The CAE consisted of two hidden layers with 32 and 16 neurons, respectively, and the model was trained for 5 epochs.

Various combinations of hyperparameter settings were explored to identify the optimal configuration. These included experimenting with the number of hidden layers, neurons per layer, batch sizes, and activation functions. The findings are presented in Figures 8a to 8d, demonstrating that the highest accuracy was achieved with two hidden layers (Figure 8a), a configuration of 32-16 neurons in hidden layers (Figure 8b), a batch size of 32 (Figure 8c), and ReLU in the hidden layers with sigmoid in the output layer (Figure 8d).

For the CNN in the hybrid module, hyperparameters were optimized through iterative experiments to achieve the best performance. The optimal configuration included two convolutional layers: the first with 64 neurons, a 3 × 3 kernel size, and ReLU activation, and the second with 32 neurons, a 2 × 2 kernel size, and ReLU activation. These layers were followed by a Flatten layer and two Dense layers, with 128 neurons (ReLU activation) and two neurons (softmax activation), respectively. The highest accuracy was achieved with a batch size of 32 and two convolutional layers, as illustrated in Figures 8e and 8f.

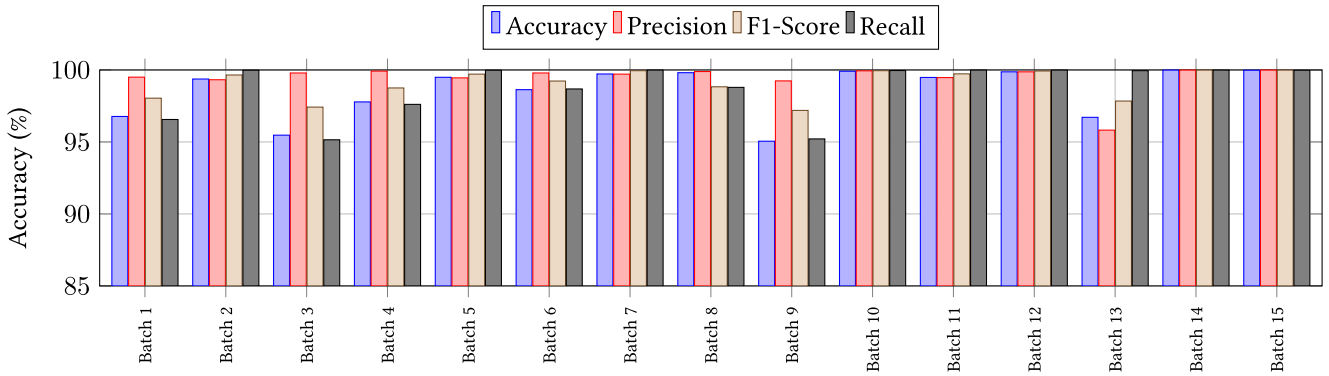


FIGURE 11. Batch-wise performance metrics CICDDOS2019.

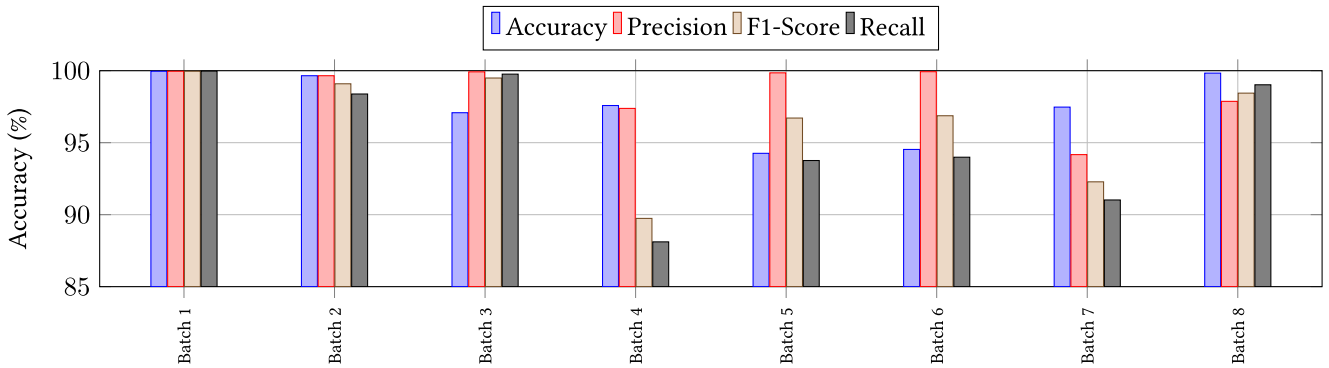


FIGURE 12. Batch-wise performance metrics CICIDS2017.

	Predicted Benign	Predicted Anomalous
Actual Benign	49072	2197
Actual Anomalous	15712	441680

(a) Batch 1

	Predicted Benign	Predicted Anomalous
Actual Benign	48182	3087
Actual Anomalous	70	457322

(b) Batch 2

	Predicted Benign	Predicted Anomalous
Actual Benign	51020	249
Actual Anomalous	20853	436539

(c) Batch 3

4	Predicted Benign	Predicted Anomalous
Actual Benign	50941	328
Actual Anomalous	10921	446471

(d) Batch 4

	Predicted Benign	Predicted Anomalous
Actual Benign	49270	1999
Actual Anomalous	83	457309

(e) Batch 5

	Predicted Benign	Predicted Anomalous
Actual Benign	50340	929
Actual Anomalous	6013	451379

(f) Batch 6

	Predicted Benign	Predicted Anomalous
Actual Benign	50887	382
Actual Anomalous	24	457368

(g) Batch 7

	Predicted Benign	Predicted Anomalous
Actual Benign	46568	440
Actual Anomalous	452	419548

(h) Batch 8

FIGURE 13. Confusion matrix: CICDDoS2019's Batch 1 - 8.

	Predicted Benign	Predicted Anomalous
Actual Benign	2756	11
Actual Anomalous	5	69995

(a) Batch 1

FIGURE 14. Confusion matrix: CICIDS2017.

VI. RESULTS AND DISCUSSION

This section presents the evaluation results of the proposed F-OSFA architecture, comparing its performance against state-of-the-art machine learning and deep learning models for both datasets (CICDDoS2019 and CICIDS2017). Both datasets were divided into multiple batches to simulate zero-day attack scenarios, as outlined in Tables 4 and 5. The CICDDoS2019 dataset was sampled to include 6.5 million instances, as shown in Table 2, and several ML and DL models were implemented for evaluation.

Figure 9 compares different classifiers on CICDDoS2019, where DL models consistently outperformed traditional ML models. The proposed F-OSFA achieved superior accuracy in original and zero-day attack scenarios, achieving 99.72% accuracy in the original dataset and 96.77% in zero-day attack simulations. Similarly, Figure 10 reports the performance of similar classifiers on the CICIDS2017 dataset. It is worth mentioning that the proposed F-OSFA again outperformed all other models, achieving 99.65% accuracy in the original dataset and 95.98% in zero-day attack scenarios.

Similarly, Table 8 presents the results for the DoS/DDoS subset of the CICIDS2017 dataset, where the proposed F-OSFA once again outperformed all other models, achieving an accuracy of 99.96% on the original dataset.

TABLE 9. Comparison of proposed F-OSFA's results with state of the art.

Reference	Technique	Dataset	Accuracy	Precision	F1 Score	Recall
[29]	KNN (PCA)	CICIDS2017	84.94	-	-	-
[29]	Similarity KNN PCA	CICIDS2017	88.29	-	-	-
[29]	LOF accuracy	CICIDS2017	91.62	-	-	-
[36]	CNN	CICIDS2017	98.61	97.05	98.09	96
[36]	LSTM	CICIDS2017	97.67	94.96	93.55	95
[36]	AE	CICIDS2017	**89.01**	-	-	-
[10]	CAE	CICIDS2017	92.45	92.46	92.45	92.45
[10]	VAE	CICIDS2017	88.73	90.15	88.63	88.73
[10]	LSTM AE	CICIDS2017	88.69	89.77	88.62	88.69
[10]	Basic AE	CICIDS2017	89.84	89.90	89.84	89.84
Whole Dataset	**Proposed F-OSFA**	**CICIDS2017**	**99.65**	**99.65**	**99.09**	**98.38**
Zero day Scenario	**Proposed F-OSFA**	**CICIDS2017**	**94.26-97.58**	**99.85**	**96.71**	**93.76**
[40]	CNN-LSTM	-	98.61	-	-	-
[41]	MC-MLDCNN	CSIC 2010 HTTP	99.36	-	-	-
[42]	ZSL-CNN	WAF,CSIC2010,Params2015	99.29	-	-	-
[10]	CAE	CICDDoS2019	95.59	-	-	-
[10]	VAE	CICDDoS2019	78.66	-	-	-
[10]	LSTM AE	CICDDoS2019	87.17	-	-	-
[10]	Basic AE	CICDDoS2019	84.61	-	-	-
[24]	DT(ID3)	CICDDoS2019	-	78	69	65
[24]	RF	CICDDoS2019	-	77	62	56
[38]	DDoSNet	CICDDoS2019	99	-	-	-
[38]	DT	CICDDoS2019	77	-	-	-
[38]	RF	CICDDoS2019	86	-	-	-
[38]	SVM	CICDDoS2019	93	-	-	-
[25]	MSCNN-AE	CICDDoS2019	99.56	98.91	98.46	98.81
[15]	Bi-LSTM	CICDDoS2019	98.18	97.93	-	99.84
[43]	FS + MLP	CICDDoS2019		91.16	79.39	79.41
[43]	DNN	CICDDoS2019	94.57	80.49	87.21	95.15
[26]	AE + MLP	CICDDoS2019	98.38	97.91	98.18	98.48
[17]	KNN	CICDDoS2019	89	89	92	91
[17]	LSTM	CICDDoS2019	98	98	97	97
[44]	CNN	CICDDoS2019	-	88.18	93.24	98.94
[44]	LSTM	CICDDoS2019	-	88.59	93.32	98.59
[44]	GRU	CICDDoS2019	-	92.22	92.31	96.5
[45]	MLP	CICDDoS2019	91.16	-	79.39	79.39
[19]	RF	CICDDoS2019	-	77	62	56
[27]	AE + SVM	CICDDoS2019	99.57	99.40	99.23	99.06
[27]	AE + LR	CICDDoS2019	99.36	98.87	98.86	98.84
[27]	AE + DNN	CICDDoS2019	98.25	97.86	94.92	96.06
[27]	DT	CICDDoS2019	97.64	98.37	95.98	93.96
[30]	DT	CICDDoS2019		84.25	83	83
[30]	RF	CICDDoS2019		89.91	90	90
[31]	KNN	CICDDoS2019	98.8	99	99	99
[31]	RF	CICDDoS2019	99	99	99	100
[14]	AE + IF	CICDDoS2019	88.98	87.92	90.61	93.48
[33]	DNN	CICDDoS2019	81.2	84.5	81.9	81.2
[33]	CNN	CICDDoS2019	85.1	87.7	85.6	85.1
Whole Dataset	**Proposed F-OSFA**	**CICDDoS2019**	**99.72**	**99.71**	**99.95**	**99.99**
Zero day Scenario	**Proposed F-OSFA**	**CICDDoS2019**	**96.77**	**99.50**	**98.04**	**96.56**

Figure 11 presents the batch-wise results of the proposed architecture on CICDDoS2019. Batch 1 of CICDDoS2019 starts with a completely zero-day attack scenario and moves iteratively with a decreasing number of zero-day attacks till batch 7, which is basically CICDDoS2019 in originality. The proposed architecture has achieved a maximum accuracy of 99.72% against CICDDoS2019 in its original form, i.e. batch 7 of table 4 and 96.77% against CICDDoS2019 in zero-day attack scenarios, i.e. batch 1. This shows the efficiency of the proposed system against possible real-world scenarios. This consistent high accuracy against different scenarios can be observed from Figure 11. Against a single attack dataset of CICDDoS2019 from batch 10 till batch 15, the proposed system has achieved an accuracy of 96.71% for syn DDoS attacks and above 99% for all other attacks. Confusion matrix as shown in Figure 13 and Figure 14 represents higher true positive rate against all attack instances of CICDDoS2019 and CICIDS2017 along with a very low False Positive Rate.

Similarly, 8 x batches have been made from CICIDS2017, as shown in Figure 12. The Proposed F-OSFA has achieved an accuracy of 94.26% - 99.83 as shown in Figure 12. As proposed, F-OSFA is specially designed for DDoS; hence when the proposed architecture is tested on the DOS /DDoS dataset of CICIDS2017 (batch 1) available in the same dataset, it achieved an accuracy of 99.96% as shown in Table 8. The proposed F-OSFA is custom-tailored as per the actual network of real-world scenarios, so when it is pitched against the complete dataset of CICIDS2017, which contains DDoS attack traffic and other network attacks, it achieves an accuracy of 99. 65% in its original form, i.e. batch 2 and 94.26% – 97.58% in zero-day attack scenarios, i.e. batch 4 - 7, as shown in Figure 12.

The evaluation results highlight the robustness and generalizability of the proposed F-OSFA, achieving consistent high accuracy across various scenarios.

The proposed architecture has been compared with state-of-the-art research in terms of accuracy as shown in Table 9, and it can be observed that the proposed F-OSFA has achieved significant improvements in results not only in the whole dataset scenarios but also in zero-day attack scenarios. The studies mentioned in the Table 9 did not perform any zero-day attack simulation, thus, our work not just advances the state of the art in terms of accuracy but also in conducting zero-day analysis and demonstrating the scheme's effectiveness on it as well.

VII. CONCLUSION AND FUTURE WORK

In this study, we proposed a novel Fog-based One Solution For All (F-OSFA) defense system to effectively address the multifaceted challenge of Distributed Denial of Service (DDoS) attacks, including zero-day attacks, in real-world scenarios. The proposed architecture integrates three distinct prongs: a hybrid deep learning and machine learning module for detecting traditional attacks, a Zero-Shot Learning (ZSL) module based on Contractive Autoencoders for identifying unknown and zero-day attacks, and a signature-based resource usage analyzer for mimicking normal traffic DDoS attacks. Through extensive experiments on CICDDoS2019 and CICIDS2017 datasets, our model demonstrated superior performance compared to state-of-the-art machine learning and deep learning approaches.

The evaluation results reveal that the F-OSFA achieved a remarkable accuracy of 99.72% on the CICDDoS2019 dataset and 99.65% on CICIDS2017 in their original forms. The model consistently outperformed other approaches in zero-day attack scenarios, with minimal accuracy drop across various configurations. This robustness highlights the generalizability and efficiency of the proposed architecture in addressing complex and evolving DDoS attack vectors. Furthermore, contractive loss and optimal threshold selection in the ZSL module achieved high detection rates for previously unseen attacks.

While the proposed system shows significant promise, several areas warrant further exploration. Future work could focus on the following directions:

- Expanding the scope of the F-OSFA framework to incorporate other types of cyber threats, such as Advanced Persistent Threats (APTs) and ransomware, to enhance its applicability in broader cybersecurity contexts.
- Generation of realistic DDoS attack dataset along with resource usage/network traffic volume data to implement signature-based resource analyzer module to detect mimic normal traffic DDoS attacks.
- Integrating federated learning to allow collaborative training across multiple fog nodes without sharing sensitive data, thus improving both model robustness and privacy.
- Exploring adaptive thresholding techniques in the ZSL module to dynamically adjust to changes in network traffic patterns and attack strategies in real-time environments.
- Enhancing scalability by deploying the F-OSFA system in large-scale distributed networks to evaluate its performance under varying network traffic and attack intensities.
- Investigating energy-efficient implementations of F-OSFA to ensure feasibility for resource-constrained environments, such as IoT ecosystems and edge computing platforms.

In conclusion, the proposed F-OSFA offers a comprehensive and scalable solution for mitigating DDoS attacks, effectively addressing the challenges posed by zero-day attacks and diverse traffic scenarios. By addressing the identified future directions, the F-OSFA framework has the potential to serve as a cornerstone in securing next-generation networks.

ACKNOWLEDGMENT

This work was Funded by the European Union under Next Generation EU, Mission 4 Component 2 - CUP

E53D23000920001. Views and opinions expressed are those of the authors only and do not necessarily reflect those of the EU or the EU REA. Neither the EU nor the granting authority can be held responsible for them.

REFERENCES

[1] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[2] N. Moustafa, K. R. Choo, I. Radwan, and S. Camtepe, "Outlier Dirichlet mixture mechanism: Adversarial statistical learning for anomaly detection in the fog," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 1975–1987, Aug. 2019.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[4] X. Sun, J. Dai, P. Liu, A. Singhal, and J. Yen, "Using Bayesian networks for probabilistic identification of zero-day attack paths," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 10, pp. 2506–2521, Oct. 2018.

[5] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Dec. 2019.

[6] K. H. Zaboon and A. A. Abdullah, "A review of the common DDoS attack: Types and protection approaches based on artificial intelligence," *Fusion, Pract. Appl.*, vol. 7, no. 1, p. 8, 2022.

[7] E. M. Maseno, Z. Wang, and H. Xing, "A systematic review on hybrid intrusion detection system," *Secur. Commun. Netw.*, vol. 2022, pp. 1–23, May 2022.

[8] Y. Ding and Y. Zhai, "Intrusion detection system for NSL-KDD dataset using convolutional neural networks," in *Proc. 2nd Int. Conf. Comput. Sci. Artif. Intell.*, Dec. 2018, pp. 81–85.

[9] M. Hajimaghsoodi and R. Jalili, "RAD: A statistical mechanism based on behavioral analysis for DDoS attack countermeasure," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2732–2745, 2022.

[10] S. Aktar and A. Yasin Nur, "Towards DDoS attack detection using deep learning approach," *Comput. Secur.*, vol. 129, Jun. 2023, Art. no. 103251.

[11] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog computing security challenges and future directions [energy and security]," *IEEE Consum. Electron. Mag.*, vol. 8, no. 3, pp. 92–96, May 2019.

[12] S. Singh, K. Kumari, S. Gupta, A. Dua, and N. Kumar, "Detecting different attack instances of DDoS vulnerabilities on edge network of fog computing using Gaussian naive Bayesian classifier," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.

[13] W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, "Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine," *IEEE Trans. Cloud Comput.*, vol. 10, no. 3, pp. 1634–1646, Jul. 2022.

[14] K. Sadaf and J. Sultana, "Intrusion detection based on autoencoder and isolation forest in fog computing," *IEEE Access*, vol. 8, pp. 167059–167068, 2020.

[15] C.-S. Shieh, W.-W. Lin, T.-T. Nguyen, C.-H. Chen, M.-F. Horng, and D. Miu, "Detection of unknown DDoS attacks with deep learning and Gaussian mixture model," *Appl. Sci.*, vol. 11, no. 11, p. 5213, Jun. 2021.

[16] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A deep-learning model for detecting network attacks," in *Proc. IEEE 21st Int. Symp. 'World Wireless, Mobile Multimedia Netw.' (WoWMoM)*, Aug. 2020, pp. 391–396.

[17] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS detection using deep learning," *Proc. Comput. Sci.*, vol. 218, pp. 2420–2429, Jan. 2023.

[18] H. Hindy, R. Atkinson, C. Tachtatzis, J.-N. Colin, E. Bayne, and X. Bellekens, "Utilising deep learning techniques for effective zero-day attack detection," *Electronics*, vol. 9, no. 10, p. 1684, Oct. 2020.

[19] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2019, pp. 1–8.

[20] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, Jan. 2020.

[21] R. Tang, Z. Yang, Z. Li, W. Meng, H. Wang, Q. Li, Y. Sun, D. Pei, T. Wei, Y. Xu, and Y. Liu, "ZeroWall: Detecting zero-day Web attacks through encoder–decoder recurrent neural networks," in *Proc. IEEE Conf. Comput. Commun.*, Jul. 2020, pp. 2479–2488.

[22] Z. Zhang, Q. Liu, S. Qiu, S. Zhou, and C. Zhang, "Unknown attack detection based on zero-shot learning," *IEEE Access*, vol. 8, pp. 193981–193991, 2020.

[23] J. Zhai, S. Zhang, J. Chen, and Q. He, "Autoencoder and its various variants," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2018, pp. 415–419.

[24] C. Tan, X. Xu, and F. Shen, "A survey of zero shot detection: Methods and applications," *Cognit. Robot.*, vol. 1, pp. 159–167, Jan. 2021.

[25] A. Singh and J. Jang-Jaccard, "Autoencoder-based unsupervised intrusion detection using multi-scale convolutional recurrent networks," 2022, *arXiv:2204.03779*.

[26] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "AE-MLP: A hybrid deep learning approach for DDoS detection and classification," *IEEE Access*, vol. 9, pp. 146810–146821, 2021.

[27] T. Fardusy, S. Afrin, I. J. Sraboni, and U. K. Dey, "An autoencoder-based approach for DDoS attack detection using semi-supervised learning," in *Proc. Int. Conf. Next-Gener. Comput., IoT Mach. Learn. (NCIM)*, Jun. 2023, pp. 1–7.

[28] B. Min, J. Yoo, S. Kim, D. Shin, and D. Shin, "Network anomaly detection using memory-augmented deep autoencoder," *IEEE Access*, vol. 9, pp. 104695–104706, 2021.

[29] T. Elmasri, N. Samir, M. Mashaly, and Y. Atef, "Evaluation of CICIDS2017 with qualitative comparison of machine learning algorithm," in *Proc. IEEE Cloud Summit*, Oct. 2020, pp. 46–51.

[30] F. Nazarudeen and S. Sundar, "Efficient DDoS attack detection using machine learning techniques," in *Proc. IEEE Int. Power Renew. Energy Conf. (IPRECON)*, Dec. 2022, pp. 1–6.

[31] A. Sharma and H. Babbar, "Evaluation and analysis: Internet of Things using machine learning algorithms for detection of DDoS attacks," in *Proc. Int. Conf. Intell. Innov. Technol. Comput., Electr. Electron. (IITCEE)*, Jan. 2023, pp. 1203–1208.

[32] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, "Fog-assisted SDN controlled framework for enduring anomaly detection in an IoT network," *IEEE Access*, vol. 6, pp. 73713–73723, 2018.

[33] M. B. Farukee, M. S. Z. Shabit, M. R. Haque, and A. H. M. S. Sattar, "DDoS attack detection in IoT networks using deep learning models combined with random forest as feature selector," in *Proc. Int. Conf. Adv. Cyber Secur.*, Penang, Malaysia. Cham, Switzerland: Springer, 2020, pp. 118–134.

[34] R. Priyadarshini and R. K. Barik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 3, pp. 825–831, Mar. 2022.

[35] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A survey of CNN-based network intrusion detection," *Appl. Sci.*, vol. 12, no. 16, p. 8162, Aug. 2022.

[36] J. Jose and D. V. Jose, "Deep learning algorithms for intrusion detection systems in Internet of Things using CIC-IDS2017 dataset," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 1, pp. 1134–1141, 2023.

[37] J. Boonchai, K. Kitchat, and S. Nonsiri, "The classification of DDoS attacks using deep learning techniques," in *Proc. 7th Int. Conf. Bus. Ind. Res. (ICBIR)*, May 2022, pp. 544–550.

[38] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS attack via deep learning," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2017, pp. 1–8.

[39] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electronics*, vol. 9, no. 6, p. 916, Jun. 2020.

[40] R. Z. Muttaqin and D. Sudiana, "Design of realtime web application firewall on deep learning-based to improve web application security," *Jurnal Penelitian Pendidikan IPA*, vol. 10, no. 12, pp. 11121–11129, Jan. 2025.

[41] N. Moarref and M. T. Sandükkaya, "MC-MLDCNN: Multichannel multilayer dilated convolutional neural networks for web attack detection," *Secur. Commun. Netw.*, vol. 2023, pp. 1–17, Dec. 2023.

[42] D. Y. Demirel and M. T. Sandikkaya, "Web based anomaly detection using zero-shot learning with CNN," *IEEE Access*, vol. 11, pp. 91511–91525, 2023.

[43] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Syst. Appl.*, vol. 169, May 2021, Art. no. 114520.

[44] D. M. Brandão Lent, M. P. Novaes, L. F. Carvalho, J. Lloret, J. J. P. C. Rodrigues, and M. L. Proença, "A gated recurrent unit deep learning model to detect and mitigate distributed denial of service and portscan attacks," *IEEE Access*, vol. 10, pp. 73229–73242, 2022.
[45] D.-C. Can, H.-Q. Le, and Q.-T. Ha, "Detection of distributed denial of service attacks using automatic feature selection with enhancement for imbalance dataset," in *Proc. Asian Conf. Intell. Inf. Database Syst.* Cham, Switzerland: Springer, Jan. 2021, pp. 386–398.

MUHAMMAD RASHID MINHAS received the B.S. degree in computer engineering from the National University of Sciences and Technology, Islamabad, and the M.S. degree in computer software from the Sir Syed CASE Institute of Technology, Islamabad, where he is currently pursuing the Ph.D. degree in electrical engineering. With over five years of research experience, his work focuses on cybersecurity, particularly developing advanced solutions for intrusion detection and prevention systems, cloud/fog computing-based internet of things (IoT), and zero-shot learning techniques for detecting zero-day attacks. His research interests include cybersecurity, machine learning, and innovative approaches to zero-day threat detection.

QAISAR M. SHAFI received the M.S. and Ph.D. degrees in information security from the National University of Sciences and Technology. He is currently an Assistant Professor with the National University of Computer and Emerging Sciences, Foundation for Advancement of Science and Technology (NUCES–FAST), Islamabad. He has more than 14 years of experience in both academics and research. He is the Lead Member of the Intelligent Systems Group (ISG). His research interests include cyber security, AI-based secure systems, intrusion detection systems, parallel and secure computational algorithm development, cloud and fog computing, and blockchain applications in security. He has been on the technical review committee of many foreign conferences.

SHOAB AHMED KHAN received the Ph.D. degree in electrical and computer engineering from Georgia Institute of Technology, Atlanta, GA, USA. He is currently a Computer and Software Engineering Professor with the College of Electrical and Mechanical Engineering, National University of Sciences and Technology (NUST). He is the Founder of the Center for Advanced Studies in Engineering (CASE) and the Center for Advanced Research in Engineering (CARE). His book on digital design was published by John Wiley and Sons and is being followed in national and international universities. He has more than 22 years of industrial experience in companies in USA and Pakistan. He is an inventor of five awarded U.S. patents and has over 260 international publications.

TAHIR AHMAD received the master's degree in computer and communication security from the School of Electrical Engineering and Computer Science (SEECS), National University of Science and Technology (NUST), Islamabad, Pakistan, in 2013, and the Ph.D. degree with a European Ph.D. Label in computer science and systems engineering from the Department of Computer Science, Bioengineering, Robotics and Systems Engineering (DIBRIS), University of Genova, Italy, in 2020. He has over 18 years of research experience in various national and international research and development organizations. His research interests include distributed systems security, with particular emphasis on understanding the security issues in the current data-driven internet-connected world and exploring practical solutions for improving their security and privacy.

SUBHAN ULLAH received the B.S. (CS) degree from the University of Malakand, Pakistan, in August 2008, the M.S. (CS) degree from the International Islamic University Islamabad, in March 2013, the Joint International Master (JIM-CS) degree from the University of Applied Science, Darmstadt, Germany, in December 2014, and the Ph.D. degree (CS) in the IoT security from the University of Klagenfurt, Austria, in collaboration with the University of Genoa, Italy, in April 2019. He is currently an Associate Professor of cybersecurity with the FAST–National University of Computer and Emerging Sciences, Islamabad, Pakistan. His research interests include cybersecurity, ML/AI, and lightweight cryptographic solutions for the IoT applications.

ATTAULLAH BURIRO received the Bachelor of Engineering (B.E.) degree in telecommunications and electronics from Mehran University of Engineering and Technology, Jamshoro, the Master of Engineering (M.E.) degree in telecommunications and electronics from the NED University of Engineering and Technology, Karachi, and the Ph.D. degree in information and communication technology (security and privacy) from the University of Trento, Italy, in February 2017. He is currently a Researcher with the Free University of Bozen-Bolzano, Italy. He has developed several secure, user-friendly, and implicit behavioral biometric-based authentication solutions for smartwatches, smartphones, and critical infrastructures. His research interests include biometrics, machine learning in cyber security, the Internet of Things (IoT), and recommender systems.

MUHAMMAD AZFAR YAQUB (Member, IEEE) received the bachelor's degree in electrical engineering from CUI, Pakistan, in 2007, the master's degree (Hons.) in CS from Lancaster University, U.K., in 2010, and the Ph.D. degree from the School of Computer Science and Engineering (SCSE), Kyungpook National University (KNU), Republic of Korea, in 2019. He is currently an Assistant Professor with the Faculty of Engineering, Free University of Bozen-Bolzano, Italy. Before this, he was with the Department of Electrical and Computer Engineering, COMSATS University Islamabad (CUI), where he taught electrical engineering courses. His research interests include intelligent networks, future internet architectures, wireless ad-hoc networks, and connected vehicles. He is an Active ACM Member serving as a TPC/reviewer for several conferences and journals.