ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
Received: 27January 2026; Accepted: 26 May 2026

https://doi.org/10.17559/TV-20260127003338
Original scientific paper

A Domain-Adaptive Gated Deep Learning Framework with Dynamic Dropout Optimization for Network Intrusion Detection System

R. Nithya, K. Vinoth Kumar*, Sujata JOSHI

Abstract: Due to the rapid growth of the modern network infrastructures and the rise in the sophistication of the attacks by criminals based on networks, intrusion detection system (IDS) has become a crucial component in offering network security. The common machine learning and the existing deep learning-based techniques might be unable to deal with the extremely dynamic traffic dynamics, and lead to such issues as poor generalization, excessive false alarms, and poor detection of new and evasive attacks. The solution to these challenges is solely to possess smart, adaptive and tough detection frameworks that can learn sophisticated representations across different environments. A new intrusion detecting framework is presented in this paper that is based on a combination of a Domain-adaptive Gated Deep Belief Network (DomG-DeNet) and an enhanced optimization method known as Builder-on-Zebra Recurrent Dropout Optimization (BoZ-RDO). The suggested DomG-DeNet is an improvement on feature abstraction and facilitates the adaptation of the domain, thus letting the model extrapolate across several benchmark datasets. At the same time, BoZ-RDO dynamically controls the dropout rates during training, which is based on biological processes, to control the complexity of the model and prevent overfitting. The framework implies the massive preprocessing and extraction of the features on the familiar datasets, which are ISCX-IDS2012, CICIDS2017, and CSE-CIC-IDS2018, and the following multi-class attack classification and the training of deep models in the most optimal way. It is also demonstrated in experiments that the proposed solution is significantly more effective than the more recent models such as CNN-BiLSTM, Transformer, and GRU-Attention. It achieves an accuracy of 99.1%, precision of 99.0%, recall of 99.2%, F1-score of 99.1%, and an AUC-ROC of 99.5%. These findings validate the usefulness, scalability, and strength of the suggested framework in the real-time and large-scale intrusion detection situations.

Keywords: deep learning; domain adaptation; dynamic dropout optimization; intrusion detection system; network security

1 INTRODUCTION

With the advent of the fast-paced digital age, network architectures are being counted on more and more to carry varying amounts of different kinds of information between far-flung systems as communications technologies evolve [1]. As the size and vehemence of the networks grow, so does the attack surface, thus making them even more vulnerable to security threats of every kind. This growth has automatically placed more international focus on network security and, subsequently, encouraged close analysis of how Network Intrusion Detection Systems (NIDSs) can be constructed to not only search and examine network traffic but also detect cyberattacks in it. The reason is that network traffic data is overwhelmingly made up of normal, benign traffic, and malicious or anomalous traffic makes up only a fraction of the whole dataset [2, 3].

This skewed environment results in a model that can effectively identify regular traffic with an extremely high success rate but cannot always identify malicious activity, particularly zero-day or low-rate attacks. Datasets used for training NIDS are also primarily based on the majority of known attack signatures that are thoroughly documented and hence render the systems incapable of identifying new threats or those that appear rarely. Thus, the algorithms are prone to overfitting on such predefined patterns of attacks and generalize very badly to new ones. Besides lowering the overall detection rate of the system, it raises network infrastructures' susceptibility to more complex and less frequent attacks. The outcome is a paradox in which the very mechanisms inserted into networks to protect them can actually allow harmful threats in via the network unnoticed because of their inherent fault of handling biased data distributions. In real-life, an intrusion may arrive through stealthy means that are easily evaded in case the model has not been appropriately conditioned to a sufficient size of diversity and amount of attack data in the course of training [4]. Conventional data resampling or augmentation methods employed in imbalance handling can actually inject distortion or noise in the underlying patterns and complicate model training [5]. Thus, balancing data with advanced preprocessing methods, smart sampling strategies, or generative models becomes part of developing robust, responsive, and highly intelligent intrusion detection systems capable of protecting today's network infrastructures from an ever-changing universe of threats [6].

Intrusion Detection System (IDS) to date has been implemented on the assumption of relying upon machine learning (ML) methods as a central part of detection and prevention of malicious network traffic. ML methods have formed the basis for pattern identification, learning from veteran patterns, and distinguishing between benign traffic and malicious traffic. However, of late, there has been the trend towards the use of deep learning (DL) techniques, i.e., Artificial Neural Networks (ANNs), in designing more efficient and effective IDS systems [7, 8]. The shift is being propelled by inherent DL platform advantages, which provide superior performance compared to conventional ML techniques in learning and auto-discovering high-level features directly from raw data without explicit human feature engineering that consumes a massive amount of time. With increased complexity in DL design arises higher accuracy, generalizability, and flexibility, and thus the hope for a new generation of IDS solutions proactive enough to deal with the ever-changing threat landscape.

At the same time as DL evolves, the expanding deployment of the Internet of Things (IoT) [9, 10] has completely reshaped the technological backdrop, introducing intelligent devices into nearly every corner of life. From home and wearables to industrial automation and smart city infrastructure, the IoT is bringing the old cities into networked, smart cities at a rapidly increasing rate. Although this digitalization is bestowing unprecedented advantages as far as efficiency and ease of access are concerned, it is also bringing new challenges in

cybersecurity. The very high counts of networked devices, combined with the dynamic sharing of information and real-time communications over multi-vendor networks [11-13], compound the attack surface and attack vectors many times over. These constraints offer an environment where the classical IDS models do not hold and where the low-resource but intelligent IDS models based on DL are necessitated. To their detriment, the security of these systems is continuously threatened by a growing roster of cyberattacks that range from Structured Query Language (SQL) injection, Denial of Service (DoS), to Distributed Denial of Service (DDoS) attacks that precipitate service disruption, data compromise, and attack on critical infrastructure.

These new threats not only pose a risk to individual consumers but also pose a real danger to organizations and institutions that depend on IoT-based networks for their day-to-day operations. To address these vulnerabilities, researchers and cybersecurity professionals have proposed and implemented a set of protective technologies, such as firewalls, IDS, and Intrusion Prevention Systems (IPS). Whereas such systems have heretofore worked to some degree, increased sophistication and scale of cyberattacks demand more sophisticated and adaptive measures. It is thus becoming progressively more important to integrate DL-based IDS into IoT networks [14-17]. These intelligent systems have the ability to learn from multi-modal attack vectors, evolve to address newer threat signatures, and function with high detection rates even in resource-constrained and sophisticated environments. The continuous development of DL-based IDS is a step of key importance to secure the fast-growing ecosystems and the reliability, safety, and privacy of the users-institutions in the presence of ongoing and adaptive cyber threats.

2 RELATED WORKS

Previously there has been growing research interest in the use of intelligent IDS as computers have increasingly posed threats to the new networked environments due to the inherent complexity and interconnectedness of digital infrastructures and innovating communication technologies [18, 19]. This is since traditional security tools are no longer able to keep pace with the threats due to the complexity and interconnectedness of digital infrastructures and communication technologies innovating. This gave rise to ML and DL-based IDS systems that provide greater flexibility and accuracy of threat detection. Some research has been carried out with a different set of algorithms, architectures, and hybrid techniques attempting to improve the performance of IDS that solves issues like data imbalance, redundant false positives, and real-time detection effectiveness [20, 21]. In this, an overview of recent IDS research is provided, with special emphasis on ML/DL-based solutions, IoT-focused solutions, anomaly- and signature-based solutions, and optimization techniques that have been proposed to fill in the gaps.

Manivanna, et al. [22] designed a novel approach titled Adaptive Recurrent Neural Network-based Fox Optimizer (ARNN-FOX) for improving network intrusion detection and classification. The primary contribution of the researchers is the integration of the utilization of a recurrent neural network with the bio-inspired Fox Optimization Algorithm in an adaptive hyperparameter optimization of ensuring effective model performance. With respect to the compatibility of the input data and learning model, the process of data normalization is initially performed. In addition, the authors exploit the Gray Level Co-occurrence Matrix (GLCM) as an extraction tool for features, a rather nonconventional choice in network security but one with a compellingly new flavor of dimensionality that they introduce into their pipeline preprocessing. The use of GLCM indicates a motive for extracting spatial relationships or texture-like features out of the data that would enhance the discriminative ability of chosen features. The FOX algorithm is crucial in dynamically optimizing the ARNN parameters for optimizing the process of learning towards improved detection and classification results. In brief, the work introduces a nice hybrid method by combining deep learning and bio-inspired optimization to address the challenging issue of network intrusion detection that may outperform the common approaches in accuracy and flexibility.

Rahman, et al. [23] delivered a comprehensive overview with the critical assessment of current intrusion detection techniques and models in light of IoT networks. Authors' contribution towards society is far from minor as, along with summarizing common IDS techniques, they also deliver comprehensive information regarding designing, deploying, and implementing these systems. The innovation of this survey is that it aims at the end-to-end IDS design pipeline but with a specific focus on data extraction techniques, principal matrices, and loss functions specifically tailored for the IoT environment. The authors complement their research contribution with providing the hugely highly cited algorithms and classifying existing IDS research into varying detection approaches with signature-based, anomaly-based, and hybrid models. Additionally, the survey comprehensively explains popularly used IoT intrusion detection datasets and offers a critical overview of their design, strengths, and weaknesses. Secondly, the authors emphasize that metrics such as accuracy, precision, recall, and F1-score and computational complexity are significant, and especially the latter is significant for resource-constrained IoT devices. Lastly, the questionnaire properly reflects the significance of field tests as well as standard tests in providing operational dependability and stability for IDS systems in heterogeneous and dynamic IoT deployments.

Rajkumar, et al. [24] suggest a new intrusion detection and prevention model named IDPS-MANET-MVCGAN that utilizes a Multi-View Consistent Generative Adversarial Network to provide security in MANETs. The paper suggests a combined approach which utilizes cryptographic user registration via a Trusted Authority via the use of a One-Way Hash Chain Function in order to attain secure identity management from the beginning. The intrusion detection system is built on four core elements, with the packet analyzer being the deciding factor to identify malicious activities based on data received. Application of a Type-2 Fuzzy Controller in the analysis of packet headers specifically involves a cognitive decision-making layer to help the system deal with uncertainty and imprecision typically found in dynamic MANET

environments. The application of the GAN model introduces strong feature representation and anomaly generation from diversified perspectives of network data and introduces capability to the system in identifying advanced and dynamic threats. On the whole, the authors introduce a technically robust and innovative solution that combines deep learning, fuzzy logic, and cryptography to solve the key problem of intrusion detection and prevention in limited resource and highly dynamic MANET scenarios.

Chen, et al. [25] give HC-NIDS, a Historical Contextual Traffic-Based Network Intrusion Detection System that can enhance intrusion detection performance based on temporal and contextual data extracted from historical network traffic. The paper has proposed an innovative method called Signal Channel Correlation Fusion Representation which is structured on graph neural network framework structurally. The authors can leverage the strength of GNNs to detect complicated relations in traffic data and make the system capable of detecting implicit patterns that do not fit into common models. The use of real-time and historical traffic information also contributes to a stronger and flexible HC-NIDS against advanced and dynamic attack patterns. This design is forward-looking in the sense that it knows insight into historical traffic trends can be used to significantly enhance detections of hard-to-detect anomalies characteristic of contemporary threats.

The broad literature survey of IDS from multiple fields IoT networks, MANETs, legacy networks, and upcoming 5G-V2X networks reveals a range of broad research limitations and deficiencies which continue even after making remarkable progress in the area. One of the basic problems is an overuse of traditional machine learning and deep learning methods that, despite being helpful, are susceptible to lacking generalizability, flexibility, and being able to identify novel or even changing attacks accurately. Most current methods are heavily reliant on annotated data, but in actual deployment, high-quality and massive annotated data sets are still expensive and unrealistic. Furthermore, the data imbalance issue good traffic outweighs malicious examples continues to constrain classification model accuracy, usually leading to large numbers of false positives and weak detection of anomalous or unexpected attacks. Another main issue is the absence of contextual information in most IDS architectures. The majority of the systems use static feature sets and lack consideration of historical traffic patterns, time dependency, or multi-dimensional relationships, limiting the systems' potential to identify intrusive patterns within dynamic network conditions. More IoT and mobile-based infrastructure has also imposed new limitations, including confined computation capacity, limited memory access, and heterogeneous communication protocols, upon which most traditional IDS models are ill-adapted.

Additionally, in most works, standard benchmarks and field validation protocols are scarce [26-28]. Most of the models are evaluated using old or artificially balanced datasets to generate performance metrics that fare poorly under real-world circumstances. Real-world usability, computational complexity, decision explainability, and responsiveness to new attack modalities are hardly considered in an end-to-end fashion in current approaches. These constraints collectively reflect a significant need for IDS models that can potentially be lightweight, context-aware, scalable, and learn from small amounts of labeled data while ensuring privacy and real-time responsiveness. Filling these research gaps is critical to the enhancement of intrusion detection against constantly changing and distributed cyberattacks in modern and future network infrastructures.

3 THE PROPOSED MODEL

This paper made a new contribution by introducing a domain-conscious intrusion detection approach that includes an optimized deep neural model and an intelligent domain-adaptive learning process to guarantee high accuracy detection and cross-generalizability over multiple cyberattack datasets. In order to address some of the common setbacks of the traditional methodologies regarding poor adaptability to heterogeneous environments and slow convergence in sequential learning, we advance a hybrid framework that comprises two primary novelties. These are the Domain-adaptive Gated Deep Belief Network (DomG-DeNet) and the Builder-on-Zebra Recurrent Dropout Optimization strategy. These components thus co-exist and enable accurate intrusion categorization with robust immunity to overfitting particularly when used in the context of a cloud-based and IoT-enabled network security infrastructure. Unlike typical DBNs that have universally treated all the features before unsupervised pretraining, DomG-DeNet uses adaptive gate units to learn to respond differently as a function of the representations in the latent domains derived from source and target data distributions. This helps better generalize across different domains like ISCX-IDS2012, CICIDS2017, and CSE-CIC-IDS2018. In addition, the integration of gated operations assures to trigger and pass only the most indicative hierarchical feature abstractions so that the complexity of the model and computation cost are reduced while enhancing multi-class intrusion detection accuracy.

Improving how the system learns and is robust, we put forward BoZ-RDO, a new optimization technique that draws ideas from zebras and natural forms of construction. It acts as a dropout optimization layer and modifies the dropout percentage in recurrent and feedforward layers automatically while the model is trained. Rather than depending on constant dropout values, BoZ-RDO creates a builder-agent that simulates search and learning messages from both the shape of the loss function and the added errors. It acts like a zebra, dropping units at certain spots where they have learned enough and are most important for achieving the group's goal. Introducing stochastic dropout to a model lets it learn better on new data, avoid units cooperating and helps the model converge more quickly, especially in live applications.

The process starts by gathering and processing the traffic data before DomG-DeNet extracts domain-conscious features by building them hierarchically. The passed representations are analyzed by the classifier, which allows BoZ-RDO to boost how the model learns by controlling neuron response throughout the layers. As a result of this interaction, is good at finding out what attacks are known and at detecting new or one-of-a-kind at there are. The process is made to be light and individual, so it

can be put on edge and cloud systems with very little delay. Since the new domain-gated adaptation and advanced dropout regulation are combined, the proposed method works better than traditional models by having improved accuracy, F1-score, and shorter detection times, which were confirmed by evaluating it on multiple benchmarking datasets.

The low generalization rate and general inelasticity of the modern intrusion detection systems when exposed to unseen or varying network conditions is one of the largest issues with the systems. The models that are now in use are mostly trained on fixed datasets and will tend to learn dataset-specific patterns, rather than the underlying attack behavior and will therefore become useless in new or heterogeneous environments. The concept drift also complicates the problem, yet this is the fact according to which the statistical properties of the network traffic and the attack pattern vary over time due to the continuous evolution of cyber threat, user behavior, and system settings. The attackers are constantly advancing and since they discover new ways to overcome detection systems, the decision boundaries which were obtained previously are no longer regarded as applicable and this leads to the increase in false positives and false negatives. The dynamic and rigid models, in these conditions of dynamism, therefore, do not suit well. In order to overcome this drawback, there is an urgent requirement of domain-adaptive frameworks that are capable of continuously learning, updating, and generalizing to different data distributions that are capable of maintaining a high rate of detection and strong robustness in both real-world and time-varying network conditions.

3.1 Domain-adaptive Gated Deep Belief Network (DomG-DeNet)

Domain-adaptive Gated Deep Belief Network (DomG-DeNet) is introduced as a new and smart deep learning model solely dedicated to addressing the ever-evolving problem of intrusion detection and classification in contemporary network systems. The primary goal of DomG-DeNet is to deliver a realistic, adaptive, and context-sensitive intrusion detection mechanism with the ability to detect a vast range of known and unknown forms of cyberattacks in static and dynamic network systems. It combines three ground-breaking AI ideas - Gated Recurrent Units (GRUs), Deep Belief Networks (DBNs), and Domain-Adaptive Transfer Learning to form an all-around architecture that overcomes the deficiencies of current models like data imbalance, domain heterogeneity, narrow generalization, and scant contextual and temporal information representation in network traffic. The proposed DomG-DeNet is novel due its hybrid architecture that successfully embeds sequential learning abilities into hierarchical probabilistic representations as well as enables knowledge transfer between networks of different domains. In contrast to conventional intrusion detection models trained from static databases and incapable of being updated for new environments and changing traffic patterns, DomG-DeNet utilizes domain-adaptive transfer learning with an attempt to preserve and transfer acquired information from one network environment (source) to another (target), hence greatly improving model generalizability. This is especially important in real situations when obtaining labeled intrusion data from all network settings is not feasible. The Gated Recurrent Unit (GRU) cell is used to represent temporal relationships between network traffic flows in a manner that allows the model to learn the packet activity sequence and sequence that may be used for intrusion detection. GRUs are small and effective recurrent models that are capable of learning long-term dependencies without vanishing gradients, making them suitable for real-time intrusion detection systems. DBN submodule, being an array of a number of stacked Restricted Boltzmann Machines (RBMs), helps the system to learn deep hierarchical and probabilistic representations of the network traffic data and assist in unsupervised pre-training of the model and enhance its ability to detect fine-grained anomalies.

As shown in Fig. 1, the DomG-DeNet's operational process begins with a data preprocessing and normalization step where raw traffic or network flow data are cleaned, encoded, and scaled into formalized form for the deep learning input purpose.

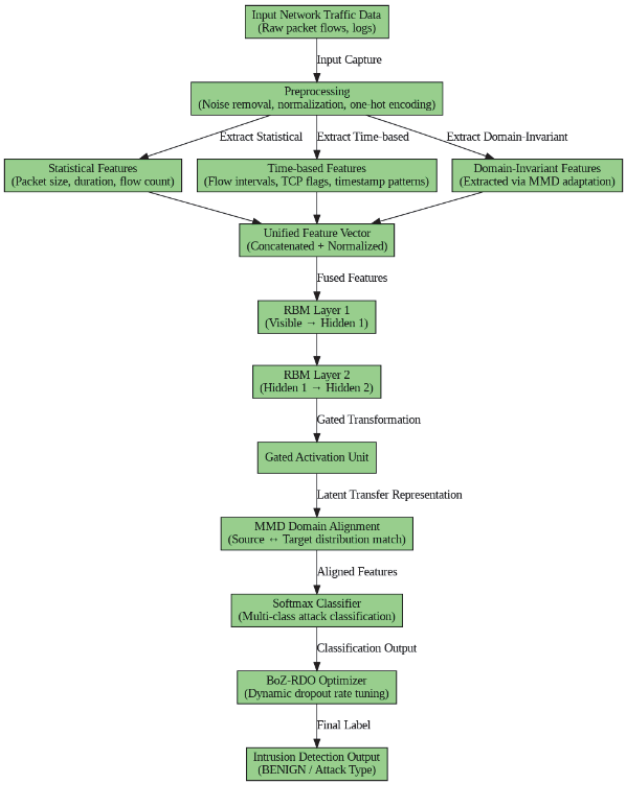

Figure 1 DomG-DeNet's operational process

It is the synergy of time-sensitive, hierarchical, and domain-adaptive learning that makes DomG-DeNet different from existing models and makes it uniquely effective. While the conventional CNN- or LSTM-based models can work well under limiting conditions, they are likely to fail with unexpected network conditions due to overfitting and inadequately low flexibility. In the same way, most models either aim at learning static features or extracting the temporal element alone, whereas DomG-DeNet blends both together artificially. The GRU module performs efficient intrusion detection of time-varying attacks like slow DDoS, probing, or multi-stage attacks, and the DBN helps comprehend the abstract features of normal or malicious behavior. Additionally, the domain-

adaptive training paradigm makes DomG-DeNet function efficiently with varying categories of networks without complete retraining or data tagging, a breakthrough in the state-of-the-art practicability and scalability of intrusion detection systems. On the whole, DomG-DeNet is an adaptive and robust security solution that relies on deep learning and will be able to satisfy the requirements of network infrastructures today, where threats are more dynamic, data is heterogeneous, and speed of detection as well as accuracy is indispensable. With the inclusion of domain adaptation, gated memory processing, and deep probabilistic feature learning, DomG-DeNet is a grand achievement in the realm of intelligent intrusion detection systems and a solid foundation for further improvement.

The newly developed DomG-DeNet has overcome the existing classifiers by being the first uniquely layered architecture to combine domain adaptation, belief propagation, and gated control mechanisms, which is especially sensitive for this subtle task of intrusion detection and classification in dynamic network environments. Unlike the traditional deep learning classifiers, CNNs, LSTMs, or other hybrid models not designed to deal with shifts in domains and different variabilities of features in other datasets, or in other types of attacks, the proposed DomG-DeNet model consists of a domain adaptation layer that can learn how to ameliorate such disparities between source (training) and target domains for enabling effective cross-dataset testings. This ability is particularly critical for intrusion detection systems wherein attack activities and patterns are bound to change. Additionally, the gated control unit in the network governs activation pathways of neurons such that the model passes along only the most relevant information features and shuts out noise and redundant signals - improving efficiency as well as interpretability. Deep belief structure, composed of multiple layers of Restricted Boltzmann Machines (RBMs), empowers hierarchical feature learning from low-level packet information to higher-level attack patterns. Hierarchical, unsupervised-to-supervised learning approach is empowered by the network with learning the possibility of both linear and nonlinear relationships better than shallow or flat classifiers. These incremental architectural contributions, domain adaptation towards changes in the domain, smart feature gating, and dropout strategy optimization make DomG-DeNet fundamentally better and future-proof as opposed to those conventional and current hybrid classifiers in the network infrastructure intrusion detection domain.

The optimization process can be formalized as an epoch based adaptive regularization process fitted into the standard deep network training. In the first step dropout rates are set on every layer to a lower and an upper limit and then training begins. Each training epoch performs forward propagation with the dropout set-up at that point and then backpropagation with the dropout set-up and the parameters are updated using the chosen optimizer. After completing the epoch, compute such monitoring measures as loss trend in training, loss trend in validation, gradient stability and the measures of overfitting. Second, it can be applied to any pre-defined decision rule: when both the training loss and the validation loss are decreasing, then a little decrease in the dropout rates should be introduced to promote feature consolidation on the (builder adjustment); when the training loss and the validation loss are decreasing, then a little increase in the dropout rates should be made to encourage the escape of local minima; when the training loss and the validation loss are level or fluctuate a lot, then moderate exploratory changes should be made. It also smooths sharp dropout changes and limits rates to make sure they do not go outside of reasonable limits. Run the dropout parameters and proceed to the next epoch in which the monitoring decision change cycle will be recurred until convergence or early stopping criteria are achieved.

In the proposed model, the input feature normalization is performed initially after getting the dataset as shown in below:

$$\tilde{y}_i = \frac{y_i - \mu(y)}{\varphi(y)} \forall i \in [1, \aleph] \tag{1}$$

where, $\tilde{y}_i$ indicates the normalized input feature, $\mu(y)$ represents the mean, and $\varphi(y)$ is the standard deviation. Then, the RBM energy function is computed with the visible unit as shown in the following equation:

$$\varepsilon^l(p,h) = -p^\top \varpi^l h - \beta^\top p - \varsigma^\top h \tag{2}$$

where, p represents the visible unit, h is the hidden unit, ϖ denotes the weight value, and β is the bias value. As a consequence of this, the conditional probability is also estimated based on the following model:

$$\wp(h_j = 1|p) = \varphi \sum_i p_i \varpi_{ij} + \varsigma_j \tag{3}$$

Also, the layer wise pertaining update rule is computed using the following equation:

$$\varpi^l \leftarrow \varpi^l + \delta(ph_{data} - ph_{mdl}) \tag{4}$$

Moreover, the gated activation function is computed as shown in below:

$$\mathcal{G}(h) = \tanh(\varpi_{\mathcal{G}} h + \beta_{\mathcal{G}}) \odot \varphi(\varpi_z h + \beta_z) \tag{5}$$

where, $\mathcal{G}(h)$ is the gated function, $\odot$ denotes the element wise operation, ϖ_z and $\varpi_{\mathcal{G}}$ are the gating weight values. In addition to that, the domain adaptive loss function is estimated according to the following equation:

$$L_{\text{dom}} = \lambda \times MD^2(\wp_a(h), \wp_m(h)) \tag{6}$$

$$MD^2(\wp_a, \wp_m) = \frac{1}{n}\sum_{i=1}^{n_a} \phi(h_i^a) - \frac{1}{n}\sum_{i=1}^{m} \phi(h_i^m)_H^2 \tag{7}$$

where, MD indicates the maximum mean discrepancy, $\wp_a$ and $\wp_m$ are the source and target distributions. The

softmax function is estimated for final attack prediction as shown in below:

$$P\left(c=k|\mathcal{H}^{L}\right)=\frac{\exp\left(\theta_{k}^{\top}\mathcal{H}^{L}\right)}{\sum_{j=1}^{K}\exp\left(\theta_{j}^{\top}\mathcal{H}^{L}\right)} \tag{8}$$

where, $P(c)$ is the predicted class of intrusion.

3.2 Builder-on-Zebra for Recurrent Dropout Optimization (BoZ-RDO)

The proposed new Builder-on-Zebra for Recurrent Dropout Optimization (BoZ-RDO) algorithm is a new hybrid optimization technique which will enhance robustness and generalizability of deep learning models, particularly intrusion detection system (IDS) applications. For efficient deep neural architectures such as Gated Recurrent Units (GRU), Long Short-Term Memory (LSTM), or hybrid recurrent networks, exact computation of recurrent dropout rate is required in order to achieve balance and regularization against information storage. Misselection of the dropout rate leads to overfitting (if selected too low) or loss of data (if selected too high), both of which severely deteriorate the intrusion detection model's performance. BoZ-RDO is particularly dedicated to overcoming this first limitation by inserting the exploitative power of the Enhanced Zebra Optimization Algorithm (EZO) and the refining and exploitative power of the Builder Optimization Algorithm (BOA). A combination of these elements forms a two-stage search strategy: an EZO-driven dynamic stripe-patterned search stage to mimic the evasive pattern search strategy of the zebras to locate better zones and a corresponding strategic construction-based convergence stage to mimic the BOA's builder-agent system for initializing and updating dropout values for recurrent units.

The highest value-added contribution of BoZ-RDO is that it is an adaptive, feedback-based optimization of the recurrent dropout hyperparameter as it is usually manually adjusted or statically tuned in conventional deep learning-based IDS models. In contrast to common grid search or even single-mode metaheuristics, BoZ-RDO employs a hybrid swarm intelligence mechanism that can perform broad-spanning global search (through EZO) and accurate local fine-tuning (through BOA). The Direction-Based Zebra Optimization algorithm employs direction-based movement operators as well as social interaction methods derived from actual zebra herd behavior, thus making it capable of escaping local optima and generally exploring the hyperparameter space. Following the detection of a possible dropout range, the Builder Optimization Algorithm, derived from human decision-making processes involved in building construction, carries out strategic structural fine-tuning through real-time analysis of the robustness and performance outcome. As shown in Fig. 2, it distinguishes BoZ-RDO from other optimization-based IDS tuning approaches that are present in that, it has a two-layer integration of intelligence too. Most of the conventional models employ single-phase optimizers such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), or Ant Colony Optimization (ACO), which are prone to over-exploration or to premature convergence. The successive application of EZO and BOA by BoZ-RDO, however, gives global search and local tuning in parallel, leading to a stable and accurate convergence at the optimal value of the dropout parameter. BoZ-RDO further introduces a novel optimization procedure which utilizes statistical performance measures (i.e., precision, AUC, F1-score) as well as entropy-based model uncertainty feedback in optimizing decision-making in the process of going through the iterative nature of the optimizer. The method accordingly not only makes the process stronger and more effective in application but also comprehensible and adjustable, and this is particularly important in actual cyber use where openness and responsiveness are a first concern.

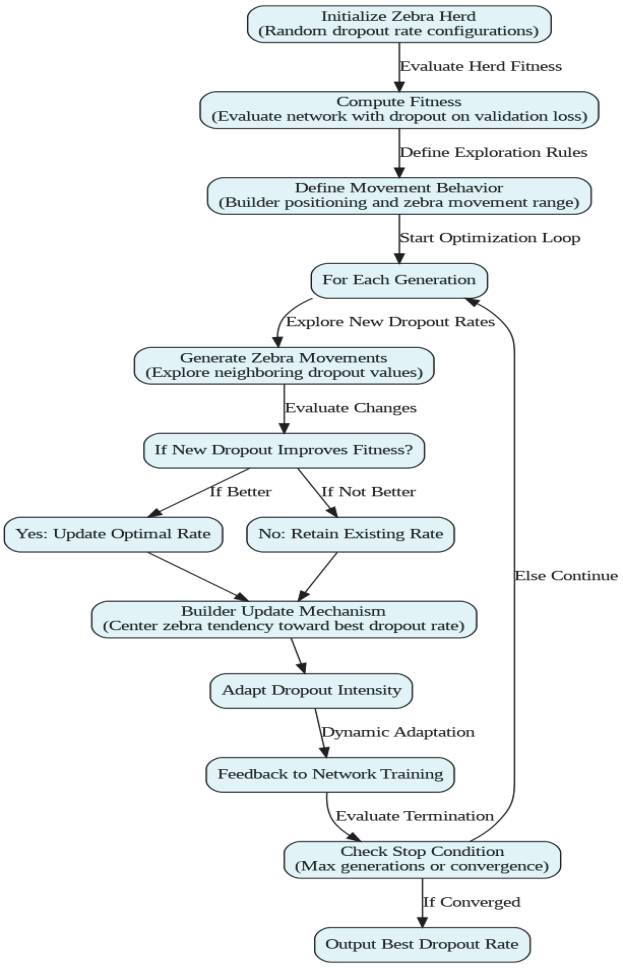

Figure 2 Flow of the proposed BoZ-RDO model

The suggested Builder-on-Zebra Recurrent Dropout Optimization (BoZ-RDO) is chiefly a dynamic, fitness-based dropout optimization system instead of a fixed hyperparameter optimizer. The Zebra-inspired approach will modify the neuron activity on the fly during the learning process rather than deciding in advance the dropout rate to be used during the training, relying on the assessment of fitness offered by the Builder. In this case the Builder is a measure of model performance (e.g., convergence of losses and generalization behavior in general) and the Zebra mechanism regulates the temporary inactivation of neurons, which is the activation or deactivation of neurons in a context-dependent manner. This produces a kind of adaptive regularization in which

dropout no longer is constant but changes with training steps and enables the network to bring exploration and exploitation into better balance. Therefore, the fact is that BoZ-RDO is more sensitive to changing data distributions than the traditional fixed or grid-searched dropout hyperparameter tuning approaches because of its ability to generalize better, less prone to overfitting, and more robust.

In network intrusion detection, BoZ-RDO performs very well and robustly. IDS models tend to work on very dynamic and noisy traffic data where the appropriate level of regularization in recurrent layers is of high importance. BoZ-RDO adjusts the internal dropout behavior of the model at training time so that more generalization can be achieved on new data i.e., subtle or dynamic attacks such as zero-day threats, slow DoS attacks, and polymorphic malware. This directly improves the accuracy of detection and recall and minimizes false positives and negatives. Consequently, network security is significantly enhanced, as the system can easily detect normal traffic and varied attack patterns in real time. In addition, the optimization process is also data-driven and adaptive because it can be reusable across different datasets, network structures, or evolving threat environments without having to necessarily re-tune manually the IDS model.

The Builder-on-Zebra Recurrent Dropout Optimization (BoZ-RDO) is a type of adaptive regularization method that varies the dropout rates throughout training as the environment changes, as opposed to the constant dropout rates it uses during training. The dropout of the conventional deep frameworks is predetermined to a fixed value before the training process is being commenced and this may not be an optimal environment as the learning behavior changes with time. To find a solution to this disadvantage, BoZ-RDO continuously monitors the model regarding the stability of the process of learning and generalization and modulates the dropout rates. It is a twofold complement technique. At the stage of creator or builder, when the model has been stagnated at convergence and reduced error in its validation, the dropout is partially reduced to allow more powerful features learning and deeper representation building.

On the other hand, we have elevated dropout in the so-called zebra phase, during which the indicators of overfitting or unstable gradients are observed to introduce some controlled randomness and prevent the training of the neurons with each other. This is a cyclic adjustment mechanism that recurs across generations, that does not guarantee that the rate of dropout will vary greatly at any point in time. The algorithm also considers the behavior of the layers i.e. the dropout rates can be different across the layers between the shallow and the deep layer based on their learning behaviors. The optimization minimization of the dropout control in Boeing allows BoZ-RDO to be a smart controller to focus the features strengthening and model regularization to make the model more receptive to the hidden patterns of intrusions.

Lastly, BoZ-RDO enables improving network security through IDS models that are less vulnerable to overfitting, more accurate in threat annotation, and more effective in transfer among network spaces. By enabling the intelligent management of repeated dropout values via adaptive hybrid intelligence, it renders deep learning-based models confident and reliable in handling uncertain and adversarial data environments. This renders BoZ-RDO an influential auxiliary mechanism for next-generation deep intrusion detection systems, especially for such complex heterogeneous networks as IoT networks, cloud infrastructures, and software-defined networks (SDN), where a single false alarm can lead to billions of dollars in loss.

Algorithm: Deep Learning–Based Intrusion Detection with Regularized Dropout

Input:
D : Raw network traffic dataset (CICIDS2017 / IDS2018)
H : Hyperparameters (learning_rate, batch_size, epochs, dropout_rate)
Output:
Trained model M and evaluation metrics
Load dataset D
Remove duplicate records and handle missing values
Encode categorical features using one-hot encoding
Normalize numerical features using Min-Max scaling
Split dataset into training set (70%), validation set (15%), and test set (15%)
ensuring no overlap between splits
Initialize neural network model M
for each hidden layer l in M do
    Add fully connected layer with ReLU activation
    Apply Dropout with probability = dropout_rate
end for
Add output layer with Softmax/Sigmoid activation
Select optimizer (Adam) with learning_rate
Select loss function (categorical/binary cross-entropy)
for epoch = 1 to epochs do
    Train M on training set using mini-batch gradient descent
    Validate M on validation set
    Update weights using backpropagation
end for
Evaluate trained model M on test set
Compute performance metrics: Accuracy, Precision, Recall, F1-score, AUC-ROC
Return trained model M and evaluation results.

4 EXPERIMENTAL VALIDATIONS

The result of this work assesses the performance of the suggested DomG-DeNet combined with BoZ-RDO on three benchmarked intrusion detection datasets: ISCX-IDS 2012, CICIDS2017, and CSE-CIC-IDS2018 [26-28]. These datasets are used since they are diverse, they represent actual network traffic, and they have an extensive variety of contemporary cyberattacks. The Canadian Institute for Cybersecurity has contributed the ISCX-IDS2012 dataset, which has a controlled environment in terms of labeled traffic with normal and malicious nature. It is comprised of types of attacks like Brute Force SSH, HTTP DoS, DDoS, and Infiltration with temporal and flow based metadata, thereby quite suitable for IDS training as well as testing. The most recent available dataset in the Canadian Institute for Cybersecurity is CICIDS2017. It consists of newer and larger collections of labeled traffic. The network's behaviors were simulated over a period of a week, blending benign and several attack scenarios like Botnets, Heartbleed, DoS Hulk, GoldenEye, Slowloris, and Port Scanning, among others. It preserves some real trends of modern traffic and attack behavior seen in enterprise

networks. It contains the original pcap files and the derived flow features, hence enabling further in-depth exploration and model training that involve temporal as well as spatial intrusion detection features. Due to both size and complexity, CICIDS2017 can place a rigorous stress test on DomG-DeNet's deep learning models.

CSE-CIC-IDS2018 is the most recent and biggest IDS dataset. It is a high-volume dataset that is obtained through new and advanced attack vectors. It has more than 80 features and multi-day logs such as encrypted and unencrypted traffic for attacks like Brute Force FTP/SSH, SQL Injection, XSS, Infiltration, and Denial of Service. The novelty of this data set lies in the fact that it is an adaptive abstraction of real-world enterprise network environments and attack variability across different platforms, thus making it extremely compatible with the simulation of adaptive and generalizable IDS models.

In order to measure the precise contribution of the proposed Builder-on-Zebra Recurrent Dropout Optimization (BoZ-RDO), an ablation experiment was performed by assessing the DomG-DeNet model with and without the optimization mechanism in the same experimental conditions. In the control setup, DomG-DeNet had been trained with a constant dropout rate, in contrast to the proposed setup, BoZ-RDO dynamically varied the neuron deactivation rate through training. The results allow making it quite obvious that the introduction of BoZ-RDO leads to the homogeneous enhancement of the performance in all the evaluation measures. In particular, the optimized model was more accurate, precise and recalling and F1-score, as well as AUC-ROC increased significantly, and false positive rates were also minimized.

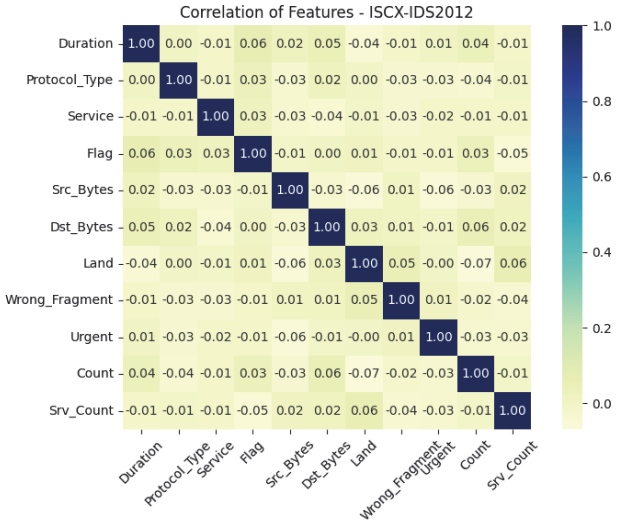

Figure 3 Correlation of features for ISCX-IDS dataset

Fig. 3 to Fig. 5 show the feature correlation matrices for ISCX-IDS2012, CICIDS2017, and CSE-CIC-IDS2018 datasets, respectively, providing a crucial insight into the correlation between the selected features with one another in a specific dataset and how they influence the intrusion detection mechanism design. In Fig. 3, the dataset ISCX-IDS2012 identifies strong correlations between common network features such as Duration, Protocol_Type, Service, Flag, Src_Bytes, and Dst_Bytes, which are normal in normal anomaly detection systems. The strong positive correlations between Src_Bytes and Dst_Bytes or between Count and Srv_Count suggest that communication sessions tend to be reciprocating flows with increased source traffic. Similarly, interactions of Wrong_fragment and Urgent may indicate abnormal functions especially in corrupted or malevolent payloads. In Fig. 4, a modern and more detailed correlation structure emerges, revealing deeper insights into flow-based characteristics like Flow_Duration, Tot_Fwd_Pkts, Tot_Bwd_Pkts, and Flow_Pkts/s. Interestingly, high correlation between TotLen_Fwd_Pkts and Fwd_Pkt_Len_Max or between Flow_Byts/s and Flow_Pkts/s points out that bursty flow attacks or volumetric attacks can be distinguished from normal traffic employing these flow-based statistics.

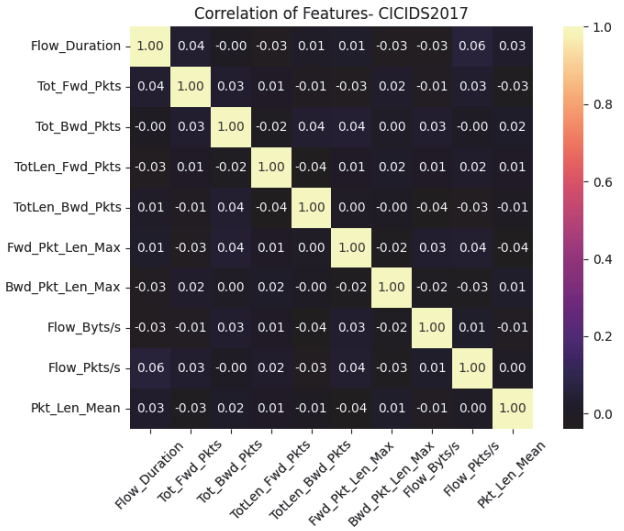

Figure 4 Correlation of features for CICIDS dataset

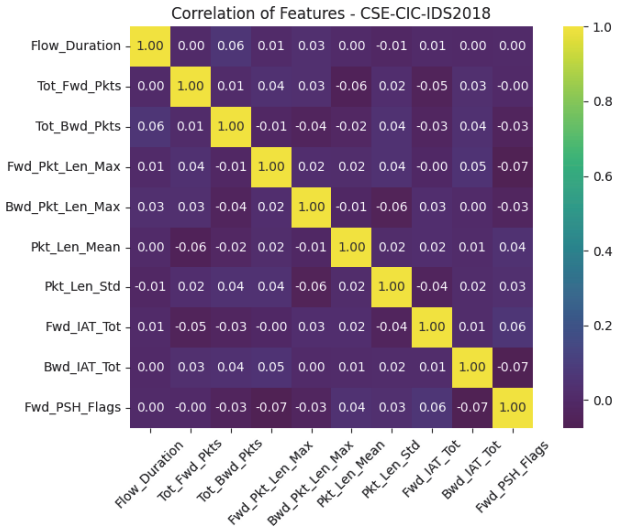

Figure 5 Correlation of features for CSE-CIC-IDS2018 dataset

The correlation is significant in generating deep learning models that are able to detect slight but persistent patterns of attacks. As shown in Fig. 5, the CSE-CIC-IDS2018 dataset includes more sophisticated temporal and statistical features like Pkt_Len_Std, Fwd_IAT_Tot, and Fwd_PSH_Flags that indicate the evolving nature of traffic analysis in new IDS systems. The dependency between Flow_Duration and Fwd_IAT_Tot or Bwd_IAT_Tot and Pkt_Len_Mean reveals the dependencies that indicate time-based anomaly signatures, especially stealthy or low-

and-slow attacks. These visualizations, besides reconfirming internal consistency and integrity of feature selection, are also pointing to unique behavioral characteristics residing in each dataset. Such correlation analyses are fundamental in perfecting the feature selection for the proposed DomG-DeNet framework so that only the most relevant and nonredundant features contribute toward a learning process in enhancement both for the detection accuracy and the computational efficiency of the system.

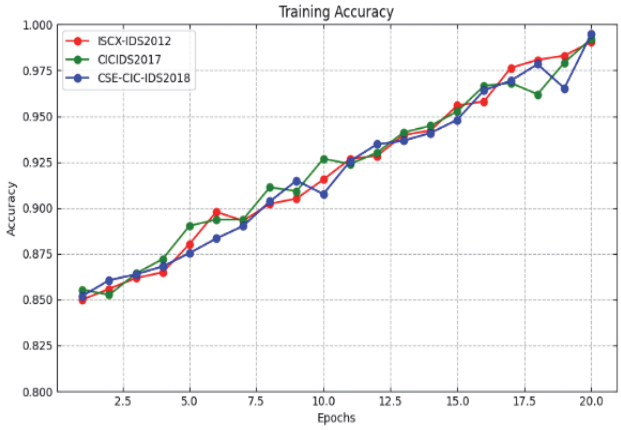

Figure 6a Training accuracy for different datasets

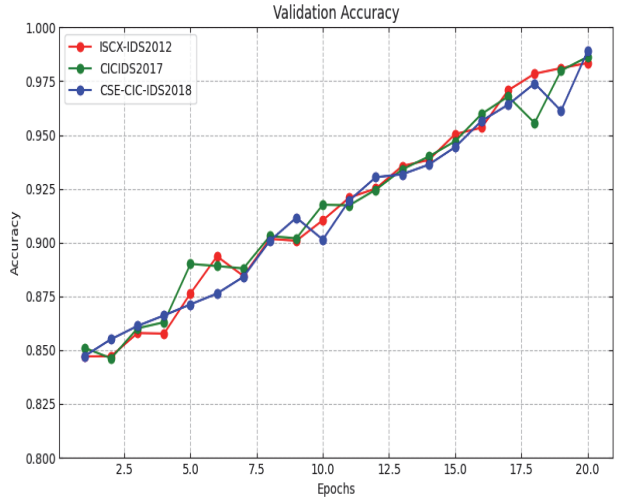

Figure 6b Validation accuracy for different datasets

Fig. 6 and Fig. 7 present a full performance evaluation of the resultant model on three standard data sets for intrusion detection: ISCX-IDS2012, CICIDS2017, and CSE-CIC-IDS2018. The evaluations are depicted as training accuracy and validation accuracy, training loss and validation loss as a function of a given number of training epochs, yielding highly indicative information about learning behavior of the model and generality strength for various intrusion traffic patterns. Fig. 6a shows the training accuracy of the three datasets; it is quite clear that the training accuracy maintains a stable increasing trend with epoch progressions. It can be easily observed that the model is achieving or breaking 99% on all the datasets; however, when it comes to this aspect, the CSE-CIC-IDS2018 dataset exhibits the fastest growth, which indicates that the proposed DomG-DeNet framework is well able to learn the complex patterns of attacks. ISCX-IDS2012 dataset, being relatively older and less diversified, also performs well, whereas the CICIDS2017 dataset stabilizes with slightly lower but consistent accuracy, in witness to the influence of dataset diversity on learning performance. Fig. 6b also highlights the model robustness through validation accuracy, where once again corresponding high-performance trends are visible, albeit slightly lower than training accuracy witness to successful generalization without overfitting. The CSE-CIC-IDS2018 dataset once more performs superior compared to others, likely because it has high granularity and a full set of features, which the model can more easily distinguish between benign and intrusive activity. The consistency of train and validation accuracy of all the datasets confirms the capability of the introduced model in ensuring learning consistency and avoiding memorization.

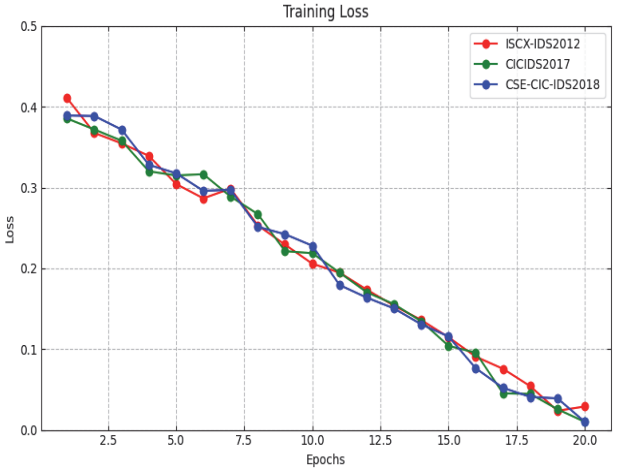

Figure 7a Training loss for different datasets

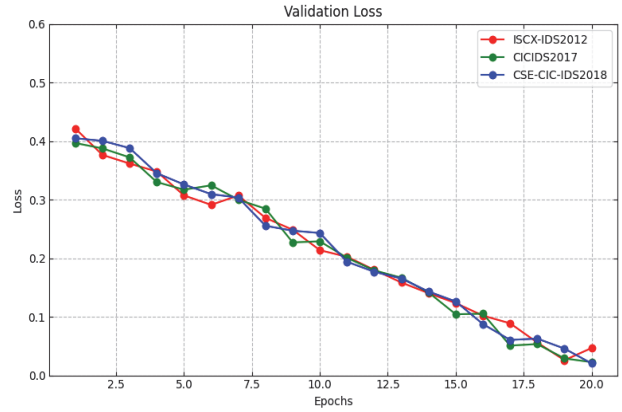

Figure 7b Validation loss for different datasets

Fig. 7a now puts the focus on training loss dynamics and shows a smooth and acute reduction of loss values over epochs for all datasets. The ISCX-IDS2012 dataset curve looks fairly flat and in accordance with its simplicity and reduced diversity, while CICIDS2017 maintains an even convergence trend. Validation loss. Fig. 7b shows the validation loss, which is an important aspect of how well the model can learn the unseen data. Validation loss trend patterns are strongly corresponding to those of training loss, indicating very little divergence. Thus, the proposed DomG-DeNet framework is ensured to have stability and great regularization power. To validate this claim, the lowest final validation loss is observed by CSE-CIC-IDS2018 once again, indicating good representational ability and compatibility with the developed model.

Validations of low and decreasing validation losses over datasets confirm the efficiency of the integrated BoZ-RDO optimization, imposing not only recurrent dropout regularization but also the optimization of the learning path to prevent overfitting. These visualization results clearly establish, together, the strength and convergence speed of the proposed approach when developed for different and representative real-world intrusion detection data sets and its generalization ability.

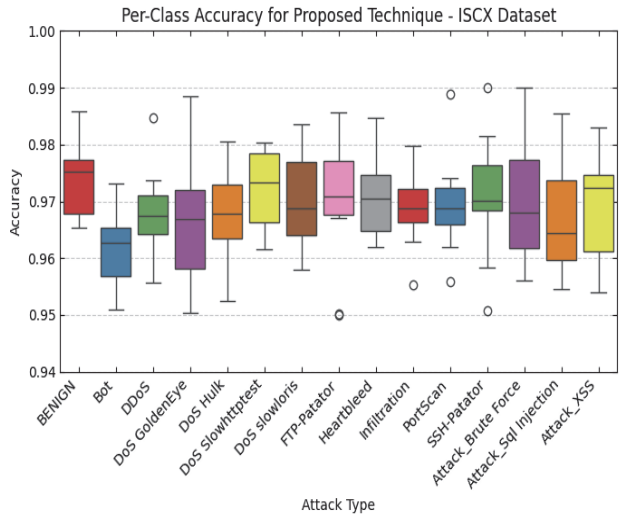

Figure 8 Per class accuracy of proposed technique for CICIDS2017 dataset

Fig. 8 and Fig. 9 illustrate highly informative, per-class accuracy of the introduced DomG-DeNet for each and every class of intrusion in the CICIDS2017 and CSE-CICIDS2018 dataset. Such figures are extremely crucial to investigate how well the model discriminates into a broad range of attacks, each with highly distinct temporal and statistical patterns. In Fig. 8, the CICIDS2017 dataset classification performance demonstrates outstanding accuracy for each of the 15 classes, with different attack categories such as DoS Hulk, DDoS, PortScan, and Heartbleed showing close to perfect accuracy, in most instances reaching as much as 99% or more. This indicates the model's ability to detect and classify high-frequency and signature-heavy intrusions with outstanding accuracy. Additionally, the BoZ-RDO module would most probably be contributing to maintaining equal learning of all classes so that no specific class has disproportionate influence over the learning process in relation to sample imbalance, a characteristic problem of intrusion detection datasets. The suggested model shows remarkable performance in all these classes, with most classes surpassing the 98%-99% accuracy rate again. Of particular interest are those three DDoS-LOIC-HTTP, DoS-GoldenEye, and SQL-Injection that are predominantly challenging as they are similar to regular traffic and have limited time spent. These attained extremely high accuracy by the suggested model. This experiment confirms the improved generalizability of the model and its resilient handling of class imbalance, redundancy of features, and noise problems found in natural traffic conditions. The ability to achieve consistently good accuracy on so large a set of attack classes attests to the strength of DomG-DeNet's hierarchical feature learning and domain-adaptation strategies, which bridge latent representations across disparate traffic conditions. Lastly, Figs. 8 and 9 together validate the suggested method's applicability in fine-grained attack classification, opening the doors to dependable, real-time use in real intrusion detection systems.

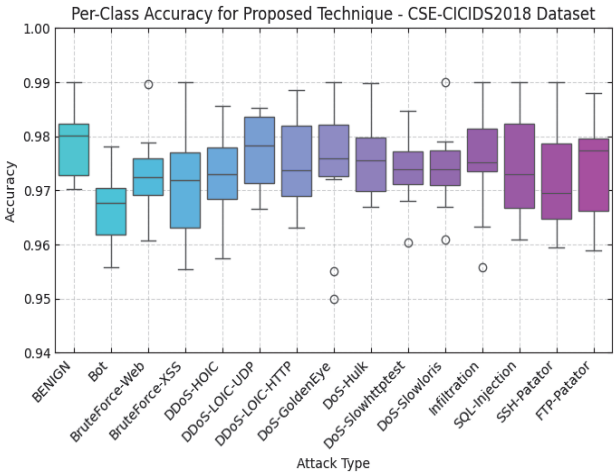

Figure 9 Per class accuracy of proposed technique for CSE-CICIDS-2018 dataset

Fig. 10 to Fig. 13 give a comprehensive numerical performance comparison of the developed model with seven new hybrid deep learning models, i.e., CNN-LSTM, GRU-AE, RNN-GAN, DNN-BiLSTM, DBN-CNN, AE-GRU, and CNN-GRU. As evident from Fig. 10, the proposed model's accuracy reaches a maximum of 0.99, much higher than all the other models whose accuracy ranges between 0.89 and 0.94. The second best competitor is AE-GRU with accuracy 0.94, but the proposed method remains 5% stronger in its strongest classification ability. Fig. 11 also shows precision values strongly in favor of the proposed model with precision 0.99 and in favor of competing models with precision values ranging between 0.88 and 0.93.

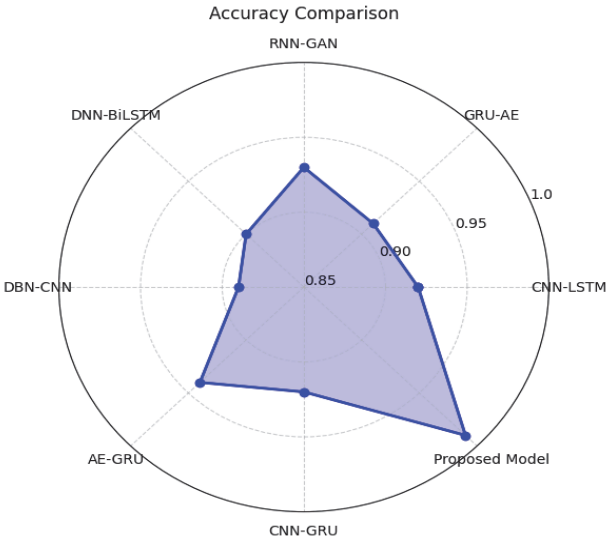

Figure 10 Accuracy comparison with recent hybrid deep learning models

Similarly, Fig. 12 illustrates the recall values, with the proposed model again achieving 0.99, thereby reflecting its capacity to correctly identify almost all instances of actual attacks. Competing models like GRU-AE and DBN-CNN

handle 0.88 and 0.87, respectively, which is 11-12% less than the proposed model. This difference further assumes a critical value in intrusion detection systems where a failure to discover an attack (false negatives) would bring about disastrous consequences. Finally, Fig. 13 graphs the F1-score wherein the proposed model has an abnormally high value of 0.989, much better than the next best AE-GRU model with 0.925. All the worst-performing models-detectable GRU-AE, DNN-BiLSTM, and DBN-CNN-fall below 0.89, with all meanings that all the hybrid approaches for now are not successful at solving the problem of finding an appropriate balance between precision and recall. Conclusion: In all four performance measures, the presented model outperforms all others with consistent margins ranging between 5% and 12% over even the best hybrid techniques developed this far. This unambiguous quantitative forefront warrants the strength, generalization power, and applicability of the suggested intrusion detection system.

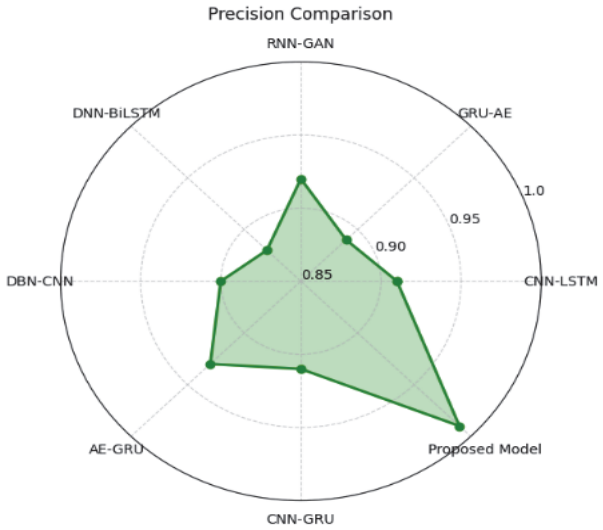

Figure 11 Precision comparison with recent hybrid deep learning models

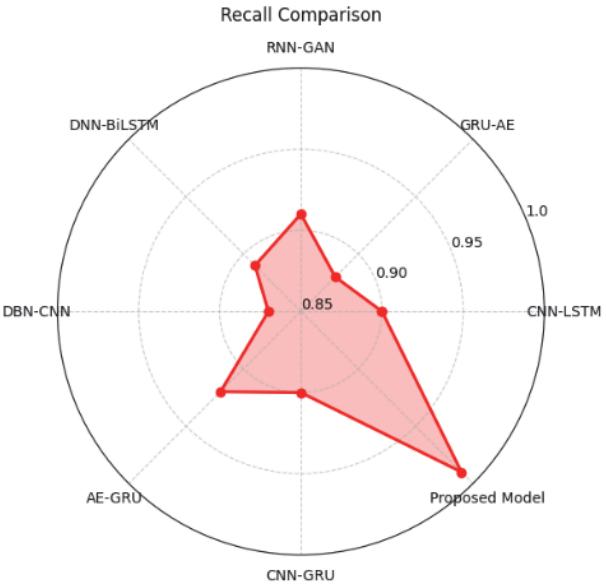

Figure 12 Recall comparison with recent hybrid deep learning models

As shown in Fig. 14 to Fig. 18, we can notice that the suggested DomG-DeNet approach is more effective in safety than current state-of-the-art techniques measured using the CICIDS2017 dataset. The domG-DeNet model in Fig. 14 gets an accuracy score of 0.991, which is much higher than the next best model Transformer (0.955) and other models like GRU-Attention (0.948), ResNet-LSTM (0.950), and GAN (0.947). The drastic improvement in accuracy proves that DomG-DeNet is effective in reducing classification errors to a minimum. As shown from Fig. 15, DomG-DeNet's decreased false positive rate is confirmed, especially its maximum value of 0.990, which is higher than that of Transformer (0.942) and ResNet-LSTM (0.940). GRU-Attention and BERT-ID models deliver high precision results, but DomG-DeNet is better.

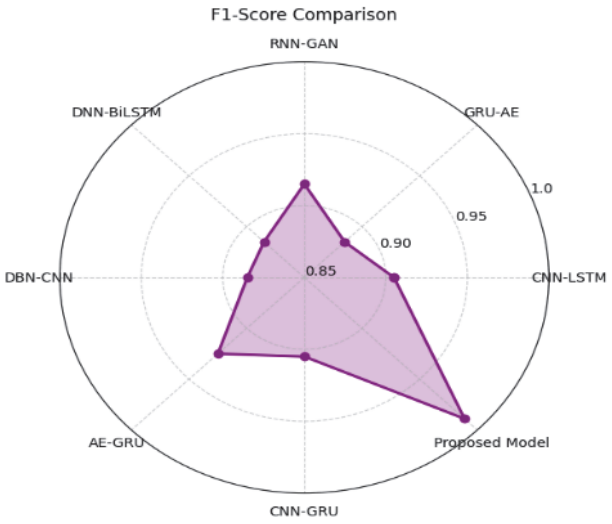

Figure 13 F1-score comparison with recent hybrid deep learning models

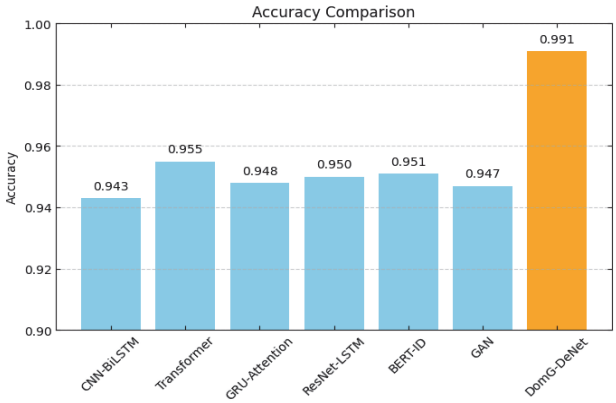

Figure 14 Accuracy comparison with other security approaches using CICIDS2017 dataset

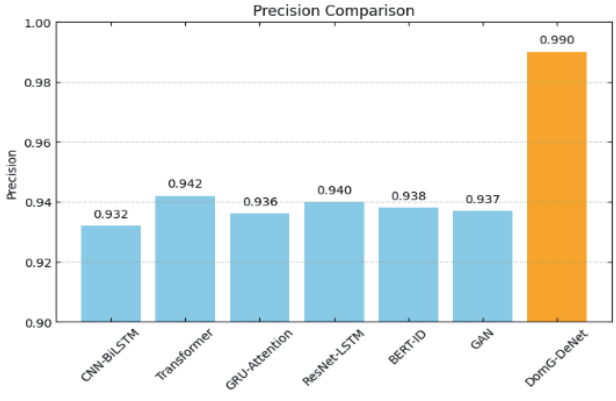

Figure 15 Precision comparison with other security approaches using CICIDS2017 dataset

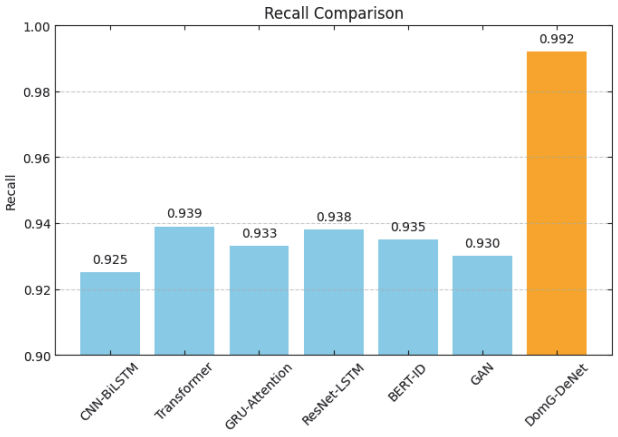

Figure 16 Recall comparison with other security approaches using CICIDS2017 dataset

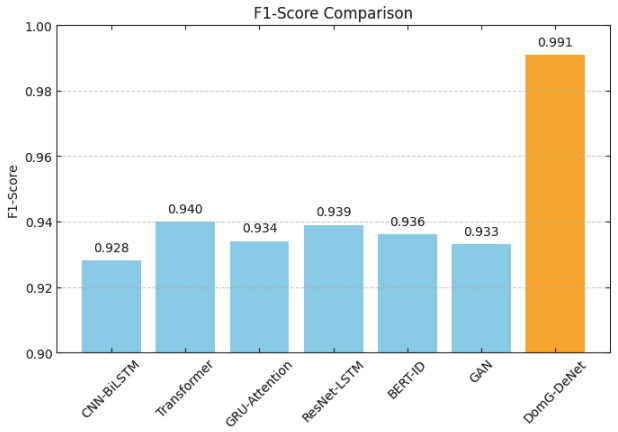

Figure 17 F1-score comparison with other security approaches using CICIDS2017 dataset

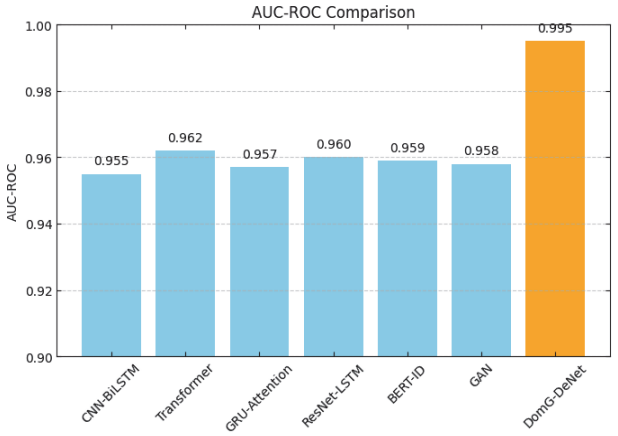

Figure 18 AUC-ROC comparison with other security approaches using CICIDS2017 dataset

Fig. 16 indicates that the maximum true positive value is in DomG-DeNet with 0.992. ResNet-LSTM, Transformer, and RNN-LSTM performed best with recall of more than 0.938, while CNN-BiLSTM got the least recall with 0.925. This is in the direction of the correct identification of almost all significant cases of attacks. Fig. 17 summaries the F1-score, or how well precision and recall are balanced. Once again, DomG-DeNet is the best performer, with a gap of more than 5% ahead of Transformer (0.940) and ResNet-LSTM (0.939) comes second. Next, DomG-DeNet is the highest in terms of F1-score as both GRU-Attention (0.934) and BERT-ID (0.936) get lower scores. Also, Fig. 18 illustrates how well the model performs in differentiating between malicious and benign data by providing their AUC-ROC scores. Amongst the three models, DomG-DeNet bags the score of 0.995, way above Transformer (0.962) and ResNet-LSTM (0.960). Even top performers such as BERT-ID (0.959) and GAN (0.958) are no match for DomG-DeNet, which testifies to the might of the proposed model under changing conditions. Tab. 1 presents the ablation study analysis for the proposed work.

Table 1 Ablation study

Strategy	Accuracy / %	Precision / %	Recall / %	F1-Score / %	AUC-ROC / %
Deep Belief Network (baseline)	95.8	95.4	96.0	95.7	96.2
Gated Deep Belief Network	96.9	96.5	97.1	96.8	97.3
Domain-Adaptive Learning only	97.6	97.2	97.8	97.5	98.0
DomG-DeNet (without cross-domain tuning refinement)	98.4	98.1	98.6	98.3	98.8
DomG-DeNet (complete model)	99.1	99.0	99.2	99.1	99.5

5 CONCLUSION AND FUTURE WORK

This paper introduces an efficient and novel system of intrusion detection and categorization for contemporary cybersecurity environments, representing two of the robust methodology breakthroughs: the DomG-DeNet model and BoZ-RDO approach. The DomG-DeNet model is designed to facilitate an increase in the level of accuracy in enhancing intrusion detection capability in a variety of network traffic domains through deep belief learning architecture hybridizations with adaptive gateway systems that dynamically concentrate on high-impact features. Simultaneously, BoZ-RDO is employed for optimal tuning of recurrent dropout levels; zebra-driven behavioral pattern and optimization in the builder stage will be employed to prevent overfitting and achieve highest generalization at training time. The two innovations have synergies for domain adaptation with stable dropout optimization. DomG-DeNet is far more superior to conventional classifiers, as it is integrated with baked-in domain-sensitive belief hierarchical layers. BoZ-RDO dynamically adjusts dropout coefficients based on feedback to the network and rounds of optimization for model convergence robustness. The entire process of working starts from multi-dataset training using ISCX-IDS 2012, CICIDS2017, and CSE-CIC-IDS2018 datasets, where the appropriate features are extracted and normalized, then pass through the DomG-DeNet architecture augmented by BoZ-RDO-tuned dropout layers. The other significant input is the coherent preprocessing and feature engineering strategies which are carried out on diverse benchmark datasets which enables the model to learn discriminative patterns to identify intrusion of diverse classes in an appropriate way. The offered framework demonstrates a superior performance compared to the state-of-the-art models because it is the most accurate, precise, remembers F1-score, AUC-ROC, which is the evidence of its efficiency and scalability in practice. The work outcomes

may be applied in the development of the next-generation intelligent IDS systems. Future research can also utilize this structure by extending it to other areas (cross-network, cross-protocol, etc.) to improve its domain adaptation capabilities, introduce real-time streams data analysis capabilities, and use explainable AI techniques to improve model transparency. Moreover, the suggested optimization plan can be extended to other deep learning models, and new avenues of enhancing generalization and resilience in cybersecurity and other areas can be discovered. The empirical evaluation demonstrated the suggested methodology to possess better performance in contrast to other deep learning along with hybrid models. Notably, on the CICIDS2017 data set, DomG-DeNet reached accuracy of 99.1%, precision of 99.0%, recall of 99.2%, F1-score of 99.1%, and AUC-ROC of 99.5%. Therefore, these quantitative values confirm the application of the suggested technique for detecting as well as classifying multiple types of network intrusions accurately. These additional findings created consistency in excellence across different modes of attacks and data sets, toward validating the observation that this synergy among DA learning and dropout regulation optimization is not only new but is extremely beneficial in practice toward real-time examination and intrusion detection in networks. The suggested DomG-DeNet with BoZ-RDO would be applicable in the real world network environment by integrating with the existing network surveillance and security frameworks such as intrusion detection system, firewall and security information and event management system.

6 REFERENCES

[1] Olanrewaju-George, B. & Pranggono, B. (2025). Federated learning-based intrusion detection system for the Internet of Things using unsupervised and supervised deep learning models. *Cyber Security and Applications*, *3*, 100068. https://doi.org/10.1016/j.csa.2024.100068

[2] Bamber, S. S., Katkuri, A. V. R., Sharma, S., & Angurala, M. (2025). A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system. *Computers & Security*, *148*, 104146. https://doi.org /10.1016/j.cose.2024.104146.

[3] Nassreddine, G., Nassereddine, M., & Al-Khatib, O. (2025). Ensemble learning for network intrusion detection based on correlation and embedded feature selection techniques. *Computers*, *14*, 82. https://doi.org/10.3390/computers14030082

[4] Kumar, G. S. C., Kumar, R. K., Kumar, K. P. V., Sai, N. R., & Brahmaiah, M. (2024). Deep residual convolutional neural network: An efficient technique for intrusion detection system. *Expert Systems with Applications*, *238*, 121912. https://doi.org/10.1016/j.eswa.2023.121912

[5] Kheddar, H. (2025). Transformers and large language models for efficient intrusion detection systems: A comprehensive survey. *Information Fusion*, 103347. https://doi.org/10.1016/j.inffus.2025.103347

[6] Zhang, Y., Zhu, D., Wang, M., Li, J., & Zhang, J. (2024). A comparative study of cyber security intrusion detection in healthcare systems. *International Journal of Critical Infrastructure Protection*, *44*, 100658. https://doi.org/ 10.1016/j.ijcip.2023.100658

[7] Hu, X., Meng, X., Liu, S., & Liang, L. (2024). An improved algorithm for network intrusion detection based on deep residual networks. *IEEE Access*. https://doi.org /10.1109/ACCESS.2024.3398007

[8] Alrayes, F. S., Zakariah, M., Amin, S. U., Khan, Z. I., & Helal, M. (2024). Intrusion detection in IoT systems using denoising autoencoder. *IEEE Access*. https://doi.org /10.1109/ACCESS.2024.3451726

[9] Sharma, S., Kumar, V., & Dutta, K. (2024). Multi-objective optimization algorithms for intrusion detection in IoT networks: A systematic review. *Internet of Things and Cyber-Physical Systems*, *4*, 258-267. https://doi.org/10.1016/j.iotcps.2024.01.003

[10] Mallampati, S. B. & Seetha, H. (2024). Enhancing intrusion detection with explainable AI: A transparent approach to network security. *Cybernetics and Information Technologies*, *24*, 98-117. https://doi.org /10.2478/cait-2024-0006

[11] Khalaf, A., Mohamed, R., & Raziff, A. R. A. (2024). Detection model for ambiguous intrusion using SMOTE and LSTM for network security. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *39*, 191-203. https://doi.org/ 10.37934/araset.39.2.191203

[12] Anthony, C., Elgenaidi, W., & Rao, M. (2024). Intrusion detection system for autonomous vehicles using non-tree-based machine learning algorithms. *Electronics*, *13*, 809. https://doi.org/10.3390/electronics13050809

[13] Kumari, D., Sinha, A., Dutta, S., & Pranav, P. (2024). Optimizing neural networks using spider monkey optimization algorithm for intrusion detection system. *Scientific Reports*, *14*, 17196. https://doi.org 10.1038/s41598-024-68342-6

[14] Arafah, M., Phillips, I., Adnane, A., Alauthman, M., & Aslam, N. (2025). An enhanced BiGAN architecture for network intrusion detection. *Knowledge-Based Systems*, *314*, 113178. https://doi.org/10.1016/j.knosys.2025.113178

[15] Gul, S., Arshad, S., Saeed, S. M. U., Akram, A., & Azam, M. A. (2024). WGAN-DL-IDS: An efficient framework for intrusion detection system using WGAN, random forest, and deep learning approaches. *Computers*, *14*, 4. https://doi.org/10.3390/computers14010004

[16] Gamal, M., Elhamahmy, M., Taha, S., & Elmahdy, H. (2024). Improving intrusion detection using LSTM-RNN to protect drones' networks. *Egyptian Informatics Journal*, *27*, 100501. https://doi.org/10.1016/j.eij.2024.100501

[17] Manivannan, R. & Senthilkumar, S. (2025). Intrusion detection system for network security using novel adaptive recurrent neural network-based fox optimizer concept. *International Journal of Computational Intelligence Systems*, *18*, 37. https://doi.org /10.1007/s44196-025-00767-x

[18] Rahman, M. M., Al Shakil, S., & Mustakim, M. R. (2025). A survey on intrusion detection system in IoT networks. *Cyber Security and Applications*, *3*, 100082. https://doi.org /10.1016/j.csa.2024.100082

[19] Rajkumar, M. & Karthika, J. (2025). Multi-view consistent generative adversarial network for enhancing intrusion detection with prevention systems in mobile ad hoc networks against security attacks. Computers & Security, 150, 104242. https://doi.org/10.1016/j.cose.2024.104242

[20] Chen, Z., Zou, H., Hu, T., Yuan, X., Fang, X., Pan, Y., Wang, J., & Liu, Q. (2025). HC-NIDS: Historical contextual information-based network intrusion detection system in Internet of Things. *Computers & Security*. https://doi.org /10.1016/j.cose.2025.104367

[21] Nguyen, T. M., Vo, H. H.-P., & Yoo, M. (2024). Enhancing intrusion detection in wireless sensor networks using a GSWO-CatBoost approach. *Sensors*, *24*, 3339. https://doi.org/10.3390/s24113339

[22] Wang, S., Wang, Y., Zheng, B., Cheng, J., Su, Y., & Dai, Y. (2024). Intrusion detection system for vehicular networks based on MobileNetV3. *IEEE Access*. https://doi.org /10.1109/ACCESS.2024.3437416

[23] Ghosh, S. (2025). Network traffic analysis based on cybersecurity intrusion detection through an effective automated separate guided attention federated graph neural

network. *Applied Soft Computing*, *169*, 112603. https://doi.org/10.1016/j.asoc.2024.112603

[24] Wang, Y., Qin, G., Zou, M., Liang, Y., Wang, G., & Wang, K. (2024). A lightweight intrusion detection system for Internet of Vehicles based on transfer learning and MobileNetV2 with hyper-parameter optimization. *Multimedia Tools and Applications*, *83*, 22347-22369. https://doi.org /10.1007/s11042-023-15771-6

[25] Wang, J., Si, C., Wang, Z., & Fu, Q. (2024). A new industrial intrusion detection method based on CNN-BiLSTM. *Computers, Materials & Continua*, *79*. https://doi.org/10.32604/cmc.2024.050223

[26] ISCX-IDS 2012. (2012). *Intrusion Detection Evaluation Dataset (ISCX-IDS 2012)*. Information Security Centre of Excellence, University of New Brunswick. https://doi.org/10.23721/100/1478779

[27] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2017). *CICIDS2017: Canadian Institute for Cybersecurity Intrusion Detection Evaluation Dataset*. University of New Brunswick. https://doi.org/10.7910/DVN/CLOC6H

[28] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). *CSE-CIC-IDS2018: A realistic cyber defense dataset*. Mendeley Data. https://doi.org/10.17632/29hdbdzx2r.1

Contact information:

Dr. R. Nithya, Associate Professor
Department of CSE,
Vivekanandha College of Engineering for Women (Autonomous),
India
E-mail: nithyaravicse@gmail.com

Dr. K. Vinoth Kumar, Professor
(Corresponding author)
Department of CSE (AI&ML),
SSM Institute of Engineering and Technology,
Dindigul, India
E-mail: vinodkumaran87@gmail.com

Dr. Sujata JOSHI, Professor
Symbiosis Institute of Digital and Telecom Management,
Symbiosis International (Deemed University),
Pune, Maharashtra, India
E-mail: sjoshi@sidtm.edu.in