Network Intrusion Detection using Combined Deep Learning Models: Literature Survey and Future Research Directions

Hamza KAMAL IDRISSI, Ali KARTIT

***Abstract*—Anomaly intrusion detection is a critical component of modern cybersecurity systems, aiming to identify and flag abnormal activities or behaviors that deviate from expected patterns within computer networks. Unlike signature-based intrusion detection systems that rely on known attack patterns, anomaly detection techniques focus on detecting unknown or novel attacks that lack predefined signatures. In recent years, machine learning and deep learning techniques have emerged as promising solutions to provide an additional layer of defense against emerging threats and zero-day attacks. This survey article provides a comprehensive review of the state of the art in network intrusion detection using ML and DL. We start by presenting an overview of the challenges and requirements associated with intrusion detection in today's dynamic network environments. We then delve into the fundamental concepts and methodologies of ML and DL, highlighting their strengths and limitations when applied to intrusion detection. We discuss the various types of network intrusion detection datasets commonly used in research, along with the preprocessing techniques employed to ensure data quality. We explore different feature selection and extraction methods that enable the effective representation of network traffic data, facilitating accurate intrusion detection. We review their architectural designs, training processes, and optimization techniques while discussing their performance in terms of detection accuracy. We highlight the current research trends and challenges in the field, including adversarial attacks, interpretability, scalability, and real-time processing. We conclude with potential future directions and recommendations for researchers and practitioners.**

***Index Terms*—Network Intrusion Detection, Anomaly Detection, Hybrid Approach, Deep Learning, Feature Extraction, Class Imbalance.**

I. Introduction

INFORMATION technology has advanced rapidly in the modern era, affecting many facets of social, professional, economic, and political life. However, this evolution has also resulted in increased network traffic load and intense use of the hardware and software infrastructure. Despite the benefits of this evolution, it also brings about risks and security issues that require the expertise of network and cybersecurity professionals.

Various security issues, including denial-of-service assaults (DoS and DDoS), compromised integrity of stored data, software intrusions that take advantage of network congestion, and other security breaches, can be led on by excessive traffic on a network. To mitigate these threats, various security mechanisms have been developed, including firewalls, data encryption, granular access control, and intrusion detection and prevention systems (IDS/IPS).

Intrusion detection systems are considered one of the most effective security solutions in the realm of computer networks. These systems are designed to immediately detect a range of suspicious behaviors and notify administrators so they may take appropriate safety precautions.

However, using traditional machine learning and deep learning approaches for anomaly-based intrusion detection poses different challenges. These include ineffective feature extraction and class imbalance, which ultimately lead to reduced detection performance. Consequently, researchers are increasingly relying on a cutting-edge approach that combines and enhances deep learning models, providing emerging possibilities for contributions.

A. Intrusion detection system

An intrusion detection system (IDS) is software that analyzes network traffic and alerts administrators when unusual behavior is detected. IDS are classified into two types: host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS). HIDS focus on a single host and are generally passive, whereas NIDS actively monitor network traffic in order to safeguard systems against network anomalies. [1]

B. Anomaly detection and signature-based detection

Intrusion Detection Systems (IDSs) adopt one of the following methods: signature-based detection or anomaly detection.

The Signature-based Detection (SD) approach compares patterns or character strings of acquired events to those of known attacks or threats. To detect prospective intrusions, this technique employs collected knowledge of specific threats and system weaknesses. It is also known as misuse detection. [2] [3]

The Anomaly-based Detection (AD), on the other hand, is based on identifying unusual behaviors in comparison to recognized actions. Over time, profiles that indicate usual or expected behaviors can be developed by monitoring daily events, network connections, hosts, or users. These static or dynamic profiles are developed based on a variety of factors such as failed connection attempts, processor usage, total number of emails sent, and quantity of data transmitted. To detect significant attacks, anomaly-based detection compares normal profiles with observed events. It is also known as behavior-based detection. [2]

Manuscript received February 10, 2024; revised June 22, 2024.

H. Kamal Idrissi is an assistant professor of STRS Laboratory, National Institute of Posts and Telecommunications (INPT), Rabat 10112, Morocco. (phone: 212-538-002855; fax: 212-537-773044; e-mail: kamalidrissi@inpt.ac.ma).

A. Kartit is a full professor of LTI Laboratory, National School of Applied Sciences of El Jadida (ENSAJ), Chouaib Doukkali University, El Jadida 24002, Morocco. (e-mail: kartit.a@ucd.ac.ma).

C. Motivations and contributions

Given the vital relevance of intrusion detection in computer networks today, classical machine learning and deep learning algorithms are limited in their detection efficiency. The use of combined deep learning solutions is gaining momentum in current research and has demonstrated various advantages.

Consequently, we are investigating novel advances in the integration of systems and clarifying their requirements. We initiated this survey research to address the crucial need to improve the efficiency of intrusion detection in order to keep IDSs resilient. Our main focus is to enhance learning approaches to increase the likelihood of successfully extracting features and addressing unbalanced class issues in a model.

The main contributions of this study can be summarized as follows:

- This study examines the latest advances in intrusion detection, utilizing machine learning and deep learning techniques.
- An assessment of current research gaps and concerns is conducted to identify areas that require further exploration.
- Finally, a comprehensive comparison of potential solutions is provided, which highlights their strengths, limitations, and potential areas for future research.

This article is structured as follows: A thorough literature analysis of traditional machine learning and deep learning techniques is presented in Section 2. The research methodology used in this survey is described in Section 3. We introduce the research issue related to the migration to combined deep learning in Section 4. A comprehensive review of combined deep learning solutions is provided in Section 5. Section 6 offers a comparative study highlighting the strengths and weaknesses of the examined models. Section 7 provides a comprehensive discussion based on the survey analysis. For each model, possible future research opportunities are discussed in Section 8. Finally, Section 9 presents the main conclusions and suggests potential directions for future research.

II. Related works

In this section of related work, we will offer a thorough overview of research that has been devoted to both the traditional method of machine learning and deep learning, to identify observed challenges and issues. Table I provides a summary of these works, with their references along with a description of the primary approaches used is also included.

The paper [4] describes an intrusion detection method based on SVM with improved training features. It uses Kullback-Leibler divergence and cross-correlation to enhance intrusion detection accuracy. The findings demonstrate that short-term intrusions in network traffic may be detected efficiently.

In this study, the researchers [5] utilized the robust NSL-KDD dataset to train a model specifically designed to identify various networking attacks. To improve the model's accuracy, they implemented the random forest algorithm. Additionally, they integrated the widely recognized technique of feature selection from data mining to improve the classification accuracy. For feature selection, they employed the Gini importance method, which proved effective in reducing the number of features used by the model. The experimental results obtained in this study demonstrated the outstanding performance of the optimized model. Not only did it showcase faster processing capabilities, but it also achieved a remarkable increase in accuracy when it came to detecting and identifying networking attacks.

This paper [6] presents an approach for developing an efficient Intrusion Detection System (IDS) using the Principal Component Analysis (PCA) and the Random Forest classification algorithm. The PCA is used to reduce the dimensionality of the dataset, while the Random Forest algorithm is employed for classification purposes. The results indicate that the proposed approach achieves higher accuracy compared to other techniques such as SVM, Naïve Bayes, and Decision Tree. The performance evaluation of the proposed method on the KDDCup99 Dataset shows good performance, a minimum time of 3.24 minutes and an accuracy rate of 96.78%.

This article [7] describes a method for detecting denial of service (DoS) attacks using a convolutional neural network (CNN) model. On the KDD dataset, the CNN model outperformed the RNN model with an accuracy of over 99% in both binary and multi-class classifications. Furthermore, the CNN model obtained an average accuracy of 91.5% for the CSE-CIC-IDS2018 dataset, whereas the RNN model earned an average accuracy of 65%. The adoption of the CNN model with adjusted parameters improves the detection of DoS attacks significantly.

[8] proposed a deep neural network model (Multi-layer perceptron) to detect and classify attacks. The model is implemented on the KDDCup 1999 dataset. Data preprocessing includes the use of One Hot Encoder and standardized Z-score. The model output provides good performance; binary classification (Normal and attack) with an overall accuracy of 99.98% and multi-class classification (Normal DoS, R2L, U2R, Probe) with an overall accuracy of 99.99%. However, this DNN solution requires a significant amount of learning data to be effective. This can be difficult to obtain in real-time production environments.

[9] proposed an intrusion detection model based on Convolutional Neural Network with a regularized multi-layer perceptron, coupled with a semi-dynamic hyperparameter tuning approach. They obtained an overall accuracy of 95.4% and 95.6% for multi-class classification. The proposed model is not particularly efficient in detecting "Zero-Day" exploits. The study was done on a single dataset "NSW-NB15" without considering dimension reduction or data balancing.

The IE-DBN model, a deep belief network model based on information entropy, is proposed in this paper [10] for network intrusion detection. To reduce dimensionality and eliminate redundant characteristics, the model employs information gain. The IE-DBN model improves convergence time, decreases overfitting, and provides improved detection accuracy with a lower false alarm rate when tested on the KDD CUP 99 intrusion detection dataset. Verification tests on other intrusion detection datasets additionally validate the IE-DBN model's high generalization capacity. In addition, The SMOTE method is used for resolving data imbalance.

The solution suggested by [11] consists of an intrusion detection system based on the BiLSTM model, which addresses

TABLE I
SUMMARY OF LITERATURE REVIEW

Ref	Year	Algorithm used	Problem solved	Dataset used	Performance Metrics
Zhang and al. [4]	2019	SVM	Low detection accuracy	Realistic Internet traffic dataset	TPR, FPR, OSR, Precision, F-score
Negandhi and al. [5]	2019	Random Forest	Low detection accuracy and high false alarm rates	NSL-KDD	Accuracy
Waskle and al. [6]	2020	Random Forest, Naive Bayes, Decision tree, SVM	Classification	KDDCup99	Performance Time, Accuracy, Error Rate
Kim and al. [7]	2020	CNN	Detecting denial of service (DoS) attacks	KDDCup99, CSE-CIC-IDS2018	Accuracy, Recall, F-score
Maithem and Alsultany [8]	2021	DNN	Low detection accuracy and high false alarm rates	KDDCup99	Accuracy, Precision, Recall, F-core, Specificity, AUC for binary classification, Average Accuracy, Precision, Recall, F-score for multi-class classification
Ashiku and Dagli [9]	2021	CNN	Classification	NSW-NB15	Accuracy
Jia and al. [10]	2021	IE-DBN model	Generalization ability and learning efficiency	KDDCup99	Accuracy, False Alarm Rate
Imrana and al. [11]	2021	BiLSTM model	High false alarm rates and low detection accuracy for U2R and R2L attacks	NSL-KDD	Accuracy, Recall, False Alarm Rate, Specificity, Precision, F-score
Kumar and Muthukumaravel [12]	2022	XGBoost Model, MLP Model	Intrusion detection	Online Dataset	Accuracy
Tahri and al. [13]	2022	Naive Bayes, SVM, KNN	Internet data security	NSL-KDD, UNSWNB15	Accuracy

the concerns of high false alarm rates and low detection accuracy for U2R and R2L attacks. The BiLSTM model outperforms previous models in terms of accuracy, recall and F-score while decreasing false alarm rates for U2R and R2L attacks.

This article [12] describes a method for intrusion detection based on deep learning approaches, notably XGBoost and MLP. The MLP model attained an accuracy of 89.5%, slightly higher than the XGBoost model's 88%. This technique effectively tackles the issue of recognizing network attacks, as proved by the use of an online dataset.

The current study by [13] employs intrusion detection systems (IDS) to address the issue of internet data security. The performance of different machine learning algorithms, including Naive Bayes, SVM and KNN, is tested in this context. The results demonstrate that the SVM algorithm performs brilliantly. The remaining research will focus on enhancing the model's processing speed and readily including it into a firewall for performing real-time assessments to enhance the current approach.

III. RESEARCH METHODOLOGY

To conduct a comprehensive and rigorous exploration of the existing studies and the latest trends and challenges in network intrusion detection using combined deep learning models, we employed Systematic Literature Review (SLR) methodology. The SLR methodology is a well-established approach that ensures the systematic identification, selection and evaluation of relevant studies from various sources, including academic databases, conference proceedings and industry reports. By following a predefined research protocol, we aimed to minimize bias and enhance the reliability and validity of our review.

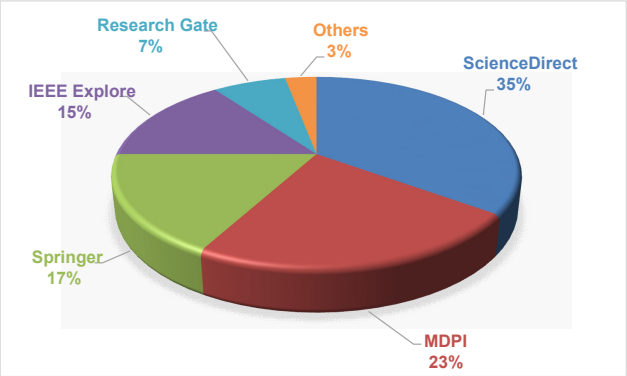

Fig. 1. Sources of research articles surveyed included in the present work

In the initial stage of our SLR, we formulated well-defined research questions to guide our search process. These questions helped us focus on many aspects such as the architecture designs, feature extraction techniques and evaluation metrics employed in the literature. Next, we conducted a comprehensive search across multiple databases, utilizing appropriate search terms and inclusion/exclusion criteria to identify relevant studies. The percentage of information sources used in this study is shown in Figure 1.

The identified studies were then screened based on their titles and abstracts, followed by a thorough full-text assessment of the selected articles. We critically analyzed each study's methodology, experimental setup and reported results to extract relevant findings and insights. Additionally, we paid close attention to the limitations and gaps identified by the authors themselves.

The findings of the selected studies were synthesized and organized to identify common trends, challenges and

future directions in the field of network intrusion detection using combined deep learning models. We considered both qualitative and quantitative aspects of the literature to provide a comprehensive overview of the current state of the art.

IV. Migration to combined deep learning solutions

Previous studies in the field of intrusion detection have mostly concentrated on the use of raw machine learning and deep learning models. However, these techniques have revealed limitations that have steered them away from the current trend in scientific research. Constraints such as reliance on manually derived features and the requirement for massive amounts of annotated data have led to the need to investigate alternatives. In this context, the transition to combined or hybrid deep learning systems has emerged as a potential scientific breakthrough.

This migration has several substantial advantages. Researchers can increase the accuracy and sophistication of visual and temporal assault detection by mixing multiple deep learning approaches, such as convolutional and recurrent neural networks. Furthermore, the combination of deep learning approaches allows for the circumvention of specific limitations by including data regularization and augmentation processes, hence enhancing model generalization and resilience.

Along with all of these benefits, the transition toward combined deep learning solutions addresses the need for intrusion detection models to be interpretable. Researchers may improve confidence and acceptability in critical scenarios by blending the explanation and visualization techniques.

As a result, the migration toward hybrid deep learning algorithms reflects an important scientific advancement in the realm of intrusion detection. It allows a departure from the limitations of traditional approaches, leveraging the synergistic benefits of various deep learning techniques, and improving the accuracy, robustness and interpretability of intrusion detection systems. As an outcome, this approach proposes novel perspectives for efficiently safeguarding computer systems against emerging threats.

V. Survey of combined deep learning solutions

A. Overview

Traditional machine learning methods are not suitable for large-scale network attack detection with this progressive enrichment of attack categories due to their limitations in terms of feature learning. Although existing classical methods based on deep learning improve detection rate (DR), they still suffer from high FPR due to insufficient feature learning.

The complex and diverse characteristics of network attacks and the unbalanced distribution of data not only limit detection efficiency, but also lead to a high false positive rate (FPR). The problem of class imbalance caused by datasets is attracting more attention due to the large discrepancy between the number of instances of different classes, which significantly reduces the detection rate.

To tackle these problems, current research is moving towards the combination of models in deep learning. Other solutions combine deep learning models with different optimization methods. Moreover, these solutions are specifically designed to improve the feature extraction process. In this section, we present a state-of-the-art of these various combined deep learning solutions based on a literature review of current research. (Table II)

B. Datasets

In this section, we provide a brief overview of several datasets that are commonly used in network intrusion detection. These datasets have been widely utilized for training, evaluating and advancing intrusion detection systems. Each dataset offers unique characteristics and challenges, allowing researchers to explore various aspects of network security.

1) KDDCup99 (Knowledge Discovery in Databases Cup 1999): The KDD Cup 1999 dataset has been a seminal dataset in the field of network intrusion detection. It was created for the Third International Knowledge Discovery and Data Mining Tools Competition, held in 1999. The KDDCup99 dataset includes a large volume of network traffic features, such as source and destination IP addresses, protocol types and connection durations. It contains both normal traffic instances and various types of attacks, including Denial of Service (DoS), Probe, User to Root (U2R) and Remote to Local (R2L). These attacks were generated using a set of predefined intrusion scenarios.

2) NSL-KDD (National Security Laboratory - Knowledge Discovery in Databases): NSL-KDD is an improved version of the KDD Cup 1999 dataset, which is used for network intrusion detection research. It addresses some limitations and challenges in the original dataset. NSL-KDD contains network traffic data generated in a simulated environment with various attack types, including Denial of Service (DoS), Probe, Remote to Local (R2L) and User to Root (U2R). It provides a labeled dataset for training and evaluating intrusion detection systems.

3) CIC-IDS2017 (Canadian Institute for Cybersecurity Intrusion Detection Evaluation Dataset 2017): CIC-IDS2017 is a network intrusion detection dataset that consists of real-world traffic captured from a controlled environment. It includes a variety of benign traffic and different types of attacks, such as DoS, DDoS, reconnaissance, and more. The dataset aims to support the development and evaluation of intrusion detection systems by providing realistic and diverse network traffic scenarios.

4) CIC-IDS2018 (Canadian Institute for Cybersecurity Intrusion Detection Evaluation Dataset 2018):: CIC-IDS2018 is another dataset provided by the Canadian Institute for Cybersecurity. It focuses on network traffic captured from a real-world industrial control systems (ICS) environment. The dataset contains both benign traffic and various attack scenarios specific to ICS, including Stuxnet, Mirai and Wannacry attacks. It is designed to aid research in securing critical infrastructure and detecting intrusions in ICS networks.

5) UNSW-NB15 (University of New South Wales Network-Baseline 2015): UNSW-NB15 is a network intrusion detection dataset that was generated by capturing raw network traffic in a controlled environment. It covers different types of attacks, including DoS, DDoS, probing and more. The dataset provides labeled data for training and evaluating intrusion detection systems and aims to support research in network security and anomaly detection.

TABLE II
SUMMARY OF THE COMBINED DEEP LEARNING MODELS

Ref	Year	Used Algorithm	Used Datasets	Performance Metrics
GSR et al. [14]	2022	RideNN-DNFN: Fisher score, RideNN, DNFN	BOT-IOT	Precision, Recall, F-measure
Fu et al. [15]	2022	DLNID: CNN+BiLSTM, ADASYN and SAE	NSL-KDD	Accuracy, Precision, Recall, F1-score and FPR
Abdullah, Abdulmajeed and Husien [16]	2022	MLIDS22: 1D CNN and LSTM	CIC2017 CIC2018	Accuracy, Precision, Recall, F1-score, FPR, TPR, TNR, FNR
Kale et al. [17]	2022	Hybrid IDS: Clustering-Kmeans, GANomaly and CNN	NSL-KDD CIC-IDS2018 TON IoT	TPR, FPR, AUC (Area under the ROC Curve)
Yoshimura et al. [18]	2022	DOC-IDS: 1D CNN, AE and three loss functions	-Reference Dataset: USTC-TFC2016 ISCX-VPN-Tor -Target Dataset: BOS 2018 CIC-IDS2017	Precision, Recall (TPR), FPR, F-measure
Hnamte and Hussain [19]	2023	DCNNBiLSTM: CNN, BiLSTM, DNN	CIC-IDS2018 EdgeIIoT	Accuracy, Loss, Inference time
Ren et al. [20]	2023	CANET: CNN, attention model, EQL v2, DNN	UNSW-NB15 NSL-KDD CIC-IDS2017 CIC-DDoS2019	Accuracy, DR, FPR
Cui et al. [21]	2023	GMM-WGAN-IDS: SAE, GMM-WGAN and CNN-LSTM	NSL-KDD UNSW-NB15	Accuracy, Precision, Recall, F1-score

6) BOT-IOT (Botnet–Internet of Things): The BOT-IOT dataset focuses on network traffic related to Internet of Things (IoT) devices. It captures traffic from a network of IoT devices infected by malware, creating a realistic scenario for studying IoT security and intrusion detection. The dataset includes both benign traffic and various IoT-based attacks, allowing researchers to develop and evaluate intrusion detection techniques specifically for IoT environments.

C. Presentation of combined deep learning models

1) Hybrid optimization enabled deep learning technique for multi-level intrusion detection [14] : This paper proposes an innovative approach based on deep learning and hybrid optimization for the multi-level intrusion detection process. Firstly, the Fisher score scheme is used to extract important features from the data. Then, a data augmentation technique is applied to increase the amount of data available, which improves model performance.

In this context, a neural network called RideNN, based on the Rider optimization algorithm, is used to perform first-level detection. categorized as normal or suspicious. In addition, the RideNN classifier is trained using the Rider social optimization algorithm (RideSOA) specially designed for this task.

In addition, a deep neural fuzzy network (DNFN) is employed to perform a second classification in which different attack types are identified and categorized. The DNFN classifier is trained using the SSSA social search algorithm, which was also developed specifically for this application.

The results obtained with the presented intrusion detection algorithm are extremely promising, outperforming other existing approaches. These performances testify to the effectiveness of this hybrid learning and optimization method for multi-level intrusion detection.

2) A Deep Learning Model for Network Intrusion Detection with Imbalanced Data [15] : In this paper, an innovative hybrid model known as DLNID is presented for network anomaly detection. The DLNID model proposes a promising method for overcoming the drawbacks of current intrusion detection algorithms. It employs a convolutional neuronal network (CNN) to extract the sequence features of data traffic, and then employs an attention mechanism to weigh these characteristics based on their importance. To capture temporal connections among data packets, the model incorporates a bidirectional long-term memory network (Bi-LSTM).

Another significant addition of the DLNID model is its ability to handle unbalanced data sets. To do this, the authors used the ADASYN algorithm to increase data and balance classes. Furthermore, a strategy for reducing data dimensionality is employed using stacked auto-encoders (SAE) in order to improve data merging.

The experimental results obtained on the reference dataset NSL-KDD demonstrate the efficiency of the DLNID model. It achieved a detection accuracy of 90.73% and an F1 score of 89.65%. These findings highlight the potential of the DLNID model for improving network anomaly detection.

3) MLIDS22- IDS Design by Applying Hybrid CNN-LSTM Model on Mixed-Datasets [16] : This study describes a novel approach for improving network intrusion detection based on a hybrid CNN-LSTM architecture. The authors concentrate on the critical dataset selection for training an anomaly-based intrusion detection system (IDS), highlighting the importance of this decision for optimal performance. They offer a new cross-dataset assessment approach and combine

the two datasets CIC-IDS2017 and CSE-CIC-IDS2018 to increase detection model performance, in order to tackle the IDS model generalization problem.

The hybrid architecture of the MLIDS22 model combines a convolution network (CNN) with a Long-Short-Term-Memory (LSTM). The CNN extracts key characteristics from the input dataset by analyzing patterns and structures, yet the LSTM enhances long-term information retention by capturing sequential dependencies. This combination enables the model to examine data efficiently and reliably identify cyber-attacks. The authors offer an effective way for enhancing intrusion detection in networks using this technique.

4) A Hybrid Deep Learning Anomaly Detection Framework for Intrusion Detection [17] : This research provides a viable answer to the problem of frequent attacks on Internet networks, calling into question the effectiveness of traditional defense techniques. The authors suggest a three-stage hybrid approach that combines deep learning with unsupervised learning. The first step employs the K-means clustering technique to differentiate between normal and obvious anomalies, minimizing the amount of data to be evaluated. The second step uses GANomaly to do semi-supervised learning, recognizing small anomalies by measuring the difference between the compressed representation of the data and its reconstruction. Finally, the third step analyzes the type of attack using a convolutional neural network (CNN) in supervised mode.

This hybrid approach has demonstrated superior results in terms of false positive rate (FPR), as well as a similar false positive rate (TPR). It overcomes the challenges associated with costly data encoding and the limited availability of atypical data.

5) DOC-IDS: A Deep Learning-Based Method for Feature Extraction and Anomaly Detection in Network Traffic [18]: This paper introduces DOC-IDS, a novel approach for detecting unknown threats in intrusion detection systems. To extract features and detect anomalies, DOC-IDS employs a deep learning model consisting of a one-dimensional convolutional network (1D CNN) and an auto-encoder. Unlike previous approaches, it requires no extensive effort to set up features or assign labels to the data. Experimental results indicate that DOC-IDS provides robust anomaly detection performance while decreasing the complexity and workload involved with data creation and labeling.

Using the DOC extraction method, which is widely used in computer vision, the DOC-IDS successfully differentiates between normal and abnormal traffic. Indeed, it is a fully automated and high-performance approach for detecting zero-day attacks, improving detection precision without the usual constraints of data creation and labeling.

6) DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System [19]: This article provides a novel approach to intrusion detection based on deep learning. The authors propose a DCNNBiLSTM architecture that combines a convolutional layer (CNN) to extract the features of input data, bidirectional recurrent networks (BiLSTMs) to predict sequences and a deep neural network (DNN) to optimize model error and loss.

The DCNNBiLSTM model is composed of upstream CNN layers, BiLSTM layers, a DNN, and finally an output layer. This architecture allows for accurate sequence prediction, quick feature extraction, and overall model enhancement. DCNNBiLSTM is an efficient method for intrusion detection, giving increased data comprehension and analysis by exploiting the abilities of deep learning, specifically by merging convolution and recurrent networks.

7) CANET: A Hierarchical CNN-Attention Model for Network Intrusion Detection [20]: The paper proposes a new hierarchical model called CANET that combines convolutional neural networks (CNN) and the attention mechanism. The proposed model integrates CA blocks (a combination of CNN and attention model) at each layer to extract spatiotemporal features for further attack identification.

The CNN is mainly divided into two parts: the convolution layer and the pooling layer. The convolution layer is used to learn the spatial characteristics of the data, while the pooling layer reduces the dimensions of the feature map and the parameters required by the subsequent layers. Next, the attention mechanism is applied to extract temporal features, and then the result is passed to the classification layer (dense layer). At the same time, to solve the problem of class imbalance, the authors propose the cost-sensitive v2 (EQL v2) method for weighting minority classes.

Extensive experiments presented in the paper demonstrate that CANET outperforms traditional machine learning algorithms by consistently improving prediction accuracy on four different datasets while achieving good performance without the need of additional data pre-processing.

8) A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data [21]: This article describes a multi-module intrusion detection approach, the WGAN-IDS, that aims to solve problems related to the detection of minor classes, the detection of unknown attacks and the reduction of false alarm rates. The system is split into three major components: feature extraction, imbalance treatment and classification.

To extract the most relevant data features, a stacked auto-encoder (SAE) is used. To improve the representation of attack and normal data, a Gaussian mixture model (GMM) and a Wasserstein antagonistic network (WGAN) are used in the treatment of imbalances. Finally, classification is performed using a convolutional neural network (CNN) combined with a short-term memory (LSTM). Based on these assessments, the GMM-WGAN-IDS method significantly improved classification accuracy on NSL-KDD and UNSW-NB15 datasets.

Table III presents the data preprocessing techniques and classification techniques employed for each combined deep learning model proposed in this survey. These techniques encompass various procedures such as class imbalance, feature extraction and dimensionality reduction.

VI. Comparative study: advantages and limitations

A. Evaluation metrics

In the context of anomaly detection, it is critical to analyze model performance in order to evaluate accuracy and efficiency. This is achieved through the use of several metrics. Accuracy is a popular metric that compares the proportion of right predictions to the total number of forecasts. However, when the classes are unbalanced, meaning there is an important difference in the quantity of both positive and negative instances, accuracy alone might be deceptive.

TABLE III
DATA PREPROCESSING AND CLASSIFICATION TECHNIQUES EMPLOYED FOR EACH COMBINED DEEP LEARNING MODEL

Model	Dim. Reduction	Class Imbalance	Feature Extraction	Classification / Detection	Classification Type
RideNN-DNFN	x	x	Score Fisher	RideNN and DNFN	Binary and Multi-class
DLNID	SAE	ADASYN	CNN	DNN (FC layer)	Binary and Multi-class
MLIDS22	Feat. reduction	ADASYN and RUS	1D-CNN (12 layers)	DNN	Multi-class
Hybrid-IDS	CNN (Maxpooling)	ADASYN	CNN (Kernels)	CNN (Log-loss)	Multi-class
DOC-IDS	x	x	1D CNN + DOC	AE (Anomaly)	Multi-class
DCNNBiLSTM	AE	SMOTE	CNN	DNN	Multi-class
CANET	x	Cost-sensitive v2 (EQL v2)	Bloc CA (CNN + attention model)	Dense layer DNN	Binary and Multi-class
GMM-WGAN-IDS	SAE	GMM-WGAN	SAE	CNN + LSTM	Multi-class

Other metrics, like precision, recall, and F1-score, are frequently utilized to solve this issue. Precision measures the proportion of true positive predictions among all positive predictions made by the model, whereas recall measures the proportion of true positive predictions among all actual positive instances in the dataset. It focuses on capturing all positive instances. The F1-score is a harmonic mean that combines accuracy and recall to provide an overall model performance metric.

$$True\ Positive\ Rate\ (Recall) = \frac{TP}{TP+FN} \quad (1)$$

$$False\ Positive\ Rate = \frac{FP}{FP+TN} \quad (2)$$

$$True\ Negative\ Rate = \frac{TN}{TN+FP} \quad (3)$$

$$False\ Negative\ Rate = \frac{FN}{FN+TP} \quad (4)$$

$$Accuracy = \frac{TN+TP}{TP+TN+FP+FN} \quad (5)$$

$$Precision = \frac{TP}{TP+FP} \quad (6)$$

$$F1\ Score = \frac{2TP}{2TP+FN+FP} \quad (7)$$

To detect intrusions effectively, both false positives and false negatives must be minimized. True Positive Rate (TPR), also known as recall or sensitivity, and False Positive Rate (FPR) are used. The proportion of intrusions accurately recognized among all real incursions is measured by TPR, whereas the fraction of non-intrusive cases wrongly labeled as intrusions is measured by FPR.

It is vital to note that the metrics used may differ based on the context of intrusion detection and research aims. Although the gathered papers employ the same metrics overall, their specific application domains may lead to variations in the metrics used.

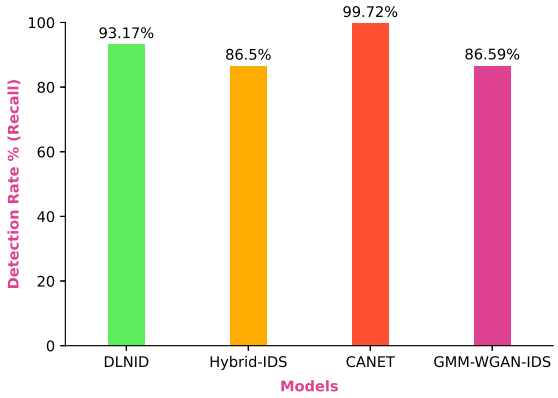

Fig. 2. Comparison based on Detection Rate of models trained with NSL-KDD Dataset

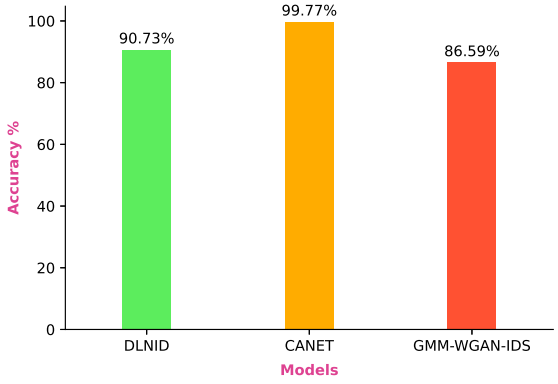

Fig. 3. Comparative analysis of Accuracy performance among models trained with NSL-KDD Dataset

B. Performance comparison of all combined models based on evaluation metrics

The performance analysis of models in Table IV highlights the importance of sharing results and comparing them. Accuracy is crucial for detection, but it is insufficient for handling class imbalance. Other metrics, like recall, F1-Score and FPR, must be selected based on the application domain's challenges and problems.

In the NSL-KDD dataset (Figures 2 and 3), we find that the CANET model performs best in terms of recall (90.72%)

TABLE IV
MODELS PERFORMANCE RESULTS

Model	Dataset	Metrics %				
		Precision	Accuracy	Recall	F-Score	FPR
DLNID	4*NSL-KDD	86.38	90.73	93.17	89.65	x
Hybrid-IDS		x	x	86.50	x	0.132
CANET		x	99.77	99.72	x	0.18
GMM-WGAN-IDS		88.55	86.59	86.59	86.88	x
MLIDS22	3*CIC-IDS2017	98.90	98.8	98.80	98.8	x
DOC-IDS		91.10	x	75.60	82.6	x
CANET		x	99.88	99.82	x	0.06
DCNNBiLSTM	3*CIC-IDS2018	100	100	x	x	x
MLIDS22		96.5	96.5	96.5	96.5	x
Hybrid-IDS		x	x	67.7	x	0.243
CANET	2*UNSW-NB15	x	89.39	98.93	x	0.87
GMM-WGAN-IDS		88.46	87.70	87.70	85.44	x
RideNN-DNFN	BOT-IOT	92.54	x	83.60	87.10	x

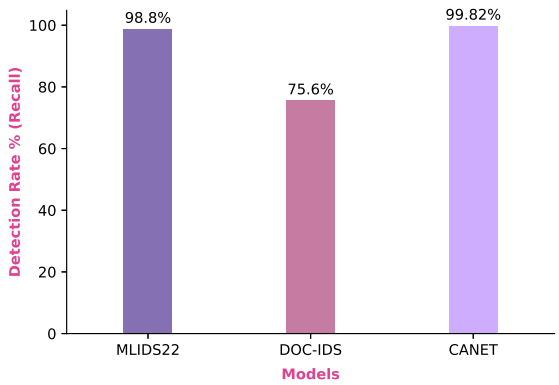

Fig. 4. Comparison based on Detection Rate of models trained with CIC-IDS2017 Dataset

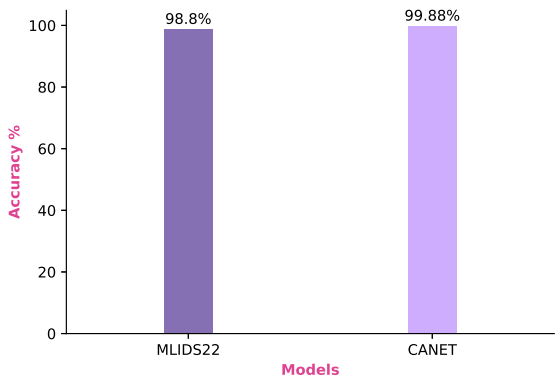

Fig. 5. Comparative analysis of Accuracy performance among models trained with CIC-IDS2017 Dataset

and accuracy (90.77%). CANET maintained its superior performance on the two additional datasets, CIC-IDS2017 and UNSW-NB15. Additionally, the false positive rates for CIC-IDS2017 and NSL-KDD are incredibly low (0.06 and 0.18, respectively), which is a positive advancement in the detection of infiltration.

Additionally, the model DLNID achieved up to 90.73% accuracy and 93.17% recall on the NSL-KDD dataset, indicating better performance rates.

The performance of the GMM-WGAN-IDS model is almost identical on the two datasets, NSL-KDD and UNSW-NB15.

The two CANET and GMM-WGAN-IDS models' successful results in the dataset UNSW-NB15 (Figures 6 and 7) demonstrate their generalizability across many datasets.

When comparing the accuracy, precision, recall, and F-score performances of the MLIDS22 model, it is clear that the test on the CIC-IDS2017 dataset (Figures 4 and 5) produced better results than CIC-IDS2018. The DCNNBiLSTM implementation on the CIC-IDS2018 dataset showed a complete accuracy of 100%.

The model Hybrid-IDS's FPR (0.243%) is relatively high on CIC-IDS2018 compared to NSL-KDD, showing that it performs well on NSL-KDD with an 86.50% detection rate as opposed to 67.7% on CIC-IDS2018.

On the other hand, the model RideNN-DNFN, tested on

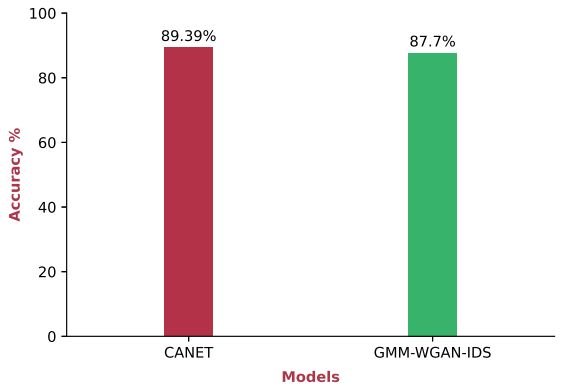

Fig. 6. Comparison based on Detection Rate of models trained with UNSW-NB15 Dataset

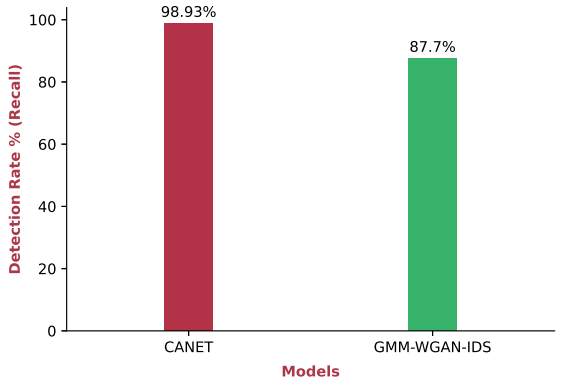

Fig. 7. Comparative analysis of Accuracy performance among models trained with UNSW-NB15 Dataset

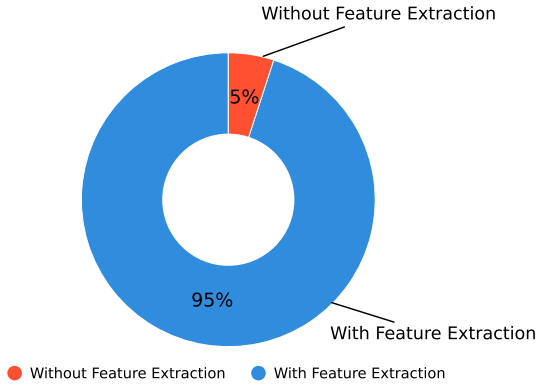

Fig. 8. The percentage of recent papers in this literature review with Feature Extraction

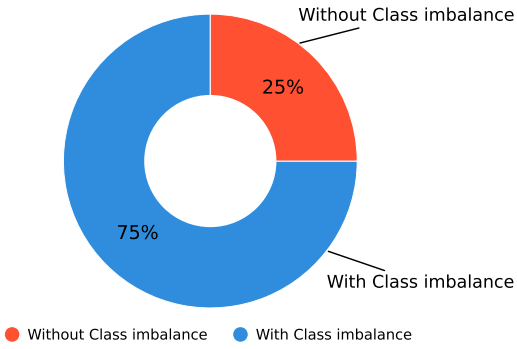

Fig. 9. The percentage of articles addressing the Class Imbalance problem in this study

the BOT-IoT dataset, produced a good precision of 92.54% in the IoT context.

Our comparative analysis of the performance of several models on the datasets listed in Table IV reveals some interesting results. The CANET model excels in terms of performance on the three datasets NSL-KDD, CIC-IDS2017 and UNSW-NB15. Hence, it is therefore widely used to learn novel attacks on new datasets. This demonstrates the careful consideration that must be given to this model.

C. Positive and negative aspects of each model

This Table V explores both the negative and positive aspects of the studied articles in order to illustrate the objectivity of the analysis. It proposes an impartial technique based on model requirements, with the goal of improving detection efficiency, complexity and computing cost. The transition to deep learning hybrid models poses challenges while also encouraging researchers to take part in this scientific adventure.

VII. Discussion

A. The particularity of a combined approach

Classical machine learning approaches identify network attacks with high accuracy but struggle with large-scale network enhancement due to limitations in distinguishing underlying properties. Existing deep learning approaches enhance detection rates but often suffer from a significant rate of false positives. The goal of the new combining techniques is to greatly enhance detection rates while reducing false positives (FPR). The CANET method, for example, outperforms typical machine learning techniques by increasing prediction accuracy and reducing FPR across four datasets without additional data preprocessing.

B. Importance of feature extraction and class imbalance

For high-dimensional network data, efficient feature extraction is a hot topic in the field of intrusion detection. [22]

Feature extraction reduces the size of the feature space by transforming the original features while retaining most of their defining attributes. [23]

The majority of the papers in this survey employ feature extraction methods for intrusion detection, including CNN, SAE and Score Fisher (Figure 8). This method effectively manages heterogeneous data, captures complicated and hierarchical patterns, automatically learns pertinent discriminative qualities, and portrays data meaningfully.

Furthermore, the problem of class imbalance caused by datasets is gaining attention due to the large difference in the number of instances of various classes, which reduces the detection rate significantly. As a result, one increasingly utilized method in the majority of studies is addressing this issue of class imbalance in new research works (Figure 9).

TABLE V
ENCOUNTERED POSITIVE AND NEGATIVE ASPECTS OF EACH MODEL DURING EXPERIMENTATION

Models	Pros	Cons
RideNN-DNFN	The model uses the Fisher score scheme for efficient feature extraction, improving intrusion detection accuracy. Its superior performance, including maximum precision, recall and F-measure, reduces false alarm rates and enhances system security.	The model's performance and accuracy depend on a varied training dataset and optimization techniques like RideSOA and SSSA, which influence both. Model performance is influenced by quality and efficiency.
DLNID	The DLNID model outperforms conventional machine learning and deep learning models in network intrusion detection, demonstrating higher accuracy, recall and F-score. It simplifies the detection process and utilizes the ADASYN algorithm to handle imbalanced data.	The DLNID model has negative aspects, such as inaccurate traffic feature extraction using CNN and high training data needs for learning sequence features using Bi-LSTM.
MLIDS22	Improved intrusion detection performance using mixed datasets, CNN+LSTM model and ALO meta-heuristic algorithm for efficient detection systems.	Data compositional differences significantly impact intrusion detection models' performance, making generalization difficult. Inter-dataset evaluations show decreased performance when dataset quality varies, questioning model robustness and adaptability to diverse environments.
Hybrid IDS	This IDS model combines supervised, unsupervised and semi-supervised learning to improve prediction accuracy and label a smaller dataset. It also identifies unexpected patterns and anomalies that traditional approaches may not detect. This approach enhances the model's ability to spot unexpected patterns in network traffic data, providing an additional layer of anomaly detection.	Resampling in CNN increases training time, limits cluster quality, and challenges the classification model due to unclear anomalies and attack labeling.
DOC-IDS	The DOC-IDS model uses open data sets without labeling, providing a practical and cost-effective approach. It has high anomaly detection performance, outperforming comparison methods and multiple classification capabilities, detecting different attack classes even when trained with normal data.	The DOC-IDS method faces limitations in open data quality and representativeness, affecting model effectiveness on specific traffic data. Flow sampling performance affects solution throughput and scalability in real environments due to the complexity of real-time data processing.
DCNNBiLSTM	The DCNNBiLSTM architecture offers an innovative approach to intrusion detection, achieving 100% accuracy on training data and 99.64% on test data, capturing spatial and temporal data characteristics for improved accuracy.	DCNNBiLSTM architectures require significant computational resources, impacting their use in resource-constrained environments. Performance relies on the quality and size of training data, with insufficient or biased data affecting generalization and intrusion detection.
CANET	The CANET model excels in detecting intrusions across diverse datasets (UNSW-NB15, NSL-KDD, CICIDS2017 and CICDDoS2019) and managing class imbalances using the cost-sensitive v2 method, reducing false positive rates and improving detection rates.	CNNs' sensitivity to spatial disturbances affects intrusion feature detection accuracy, requiring robust strategies to mitigate residual sensitivity. Attention errors impact performance, causing erroneous distributions and requiring mechanisms to correct them.
GMM-WGAN-IDS	GMM-WGAN-IDS improves accuracy, detects novel attacks and efficiently handles unbalanced data by subsampling majority data and generating synthetic minority data.	The proposed system uses complex algorithms such as SAE, WGAN, etc, requiring specialized expertise and resources for implementation and training.

C. Why CNNs are mostly used in combined deep learning solutions?

CNNs, or Convolutional Neural Networks, are commonly used in network intrusion detection (Figure 10) for feature extraction due to their ability to effectively capture spatial dependencies in data. These networks employ small filters that scan the input data, allowing them to detect local patterns present in network traffic. These patterns, such as specific byte sequences or traffic behavior, can indicate various types of network intrusions. Moreover, CNNs exhibit robustness to slight translations or shifts in the input data, enabling them to identify patterns regardless of their precise location within the data stream. This is particularly useful in network traffic analysis, as intrusion patterns can occur at different positions in network packets, and CNNs excel at effectively capturing them.

CNNs are designed to automatically learn relevant features from raw data. They are effective in capturing local patterns and hierarchical structures in the data, making them suitable for intrusion detection where specific patterns may indicate malicious behavior. CNNs can maintain spatial invariance of extracted features, meaning they are insensitive to variations in pattern positions within the data. In the field of intrusion detection, this allows for the detection of attacks, even if they are concealed in different parts of the data.

Data used for intrusion detection, such as network event logs, can be voluminous and complex. CNNs are effective in handling such large-scale data by exploiting local structure and using convolution operations to reduce the dimensionality of the data.

Additionally, CNNs use shared filters to extract features from different parts of the data, significantly reducing the number of parameters to be trained. This parameter sharing property is crucial when training data is limited. Moreover, CNNs share parameters across different regions of the input data, resulting in a reduction in the number of trainable parameters. This parameter sharing property enhances the efficiency of the network. In the realm of network traffic analysis, parameter pooling enables the CNN to generalize well to different parts of the traffic by improving its ability to detect intrusions even in unseen data.

In summary, CNNs offer significant advantages in intrusion detection due to their ability to extract discriminative features, handle large-scale data, maintain the spatial invariance and exploit deep learning. However, the choice of architecture will depend on the characteristics of the data, specific goals of intrusion detection and system constraints.

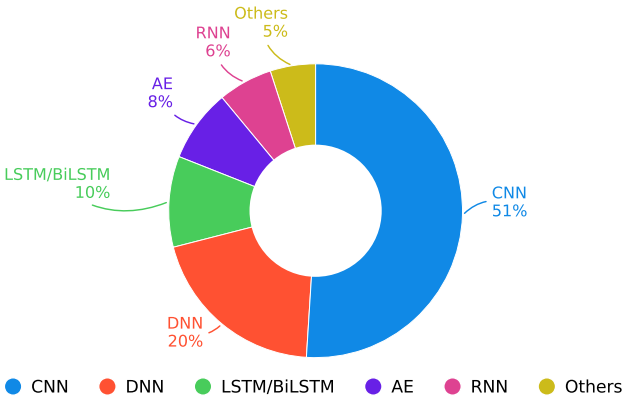

Fig. 10. The most frequently used algorithms in combined Deep Learning solutions

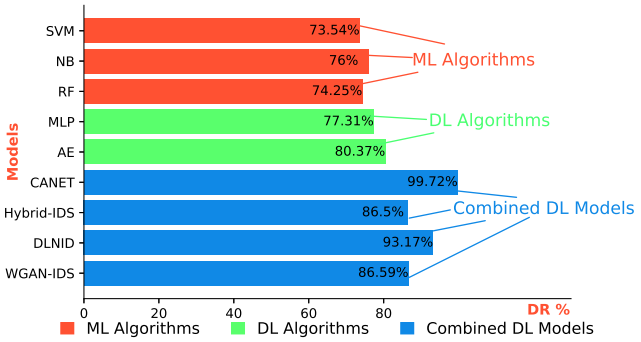

Fig. 11. Comparison based on DR between Combined DL Models and ML/DL Algorithms Trained with NSL-KDD Dataset

D. Comparisons with other methods

Based on the diagram in Figure 11, traditional approaches such as Support Vector Machine (SVM), Random Forest (RF), and Naive Bayes (NB) exhibit a limited detection rate, not surpassing 76%. Similarly, classical deep learning models achieve a detection rate of approximately 77% and 80% with Multi-layer Perceptron (MLP) and Autoencoders (AE) [21] [15]. However, the study reveals that the implementation of combined deep learning models [20] [21] gives significantly superior results, boasting an impressive detection rate of up to 99.72% with the CANET model. This substantial improvement demonstrates the effectiveness of employing a combined approach for network intrusion detection, as compared to traditional machine learning and classical deep learning techniques.

The second diagram in Figure 12 compares the performance of combined deep learning models and traditional machine learning models based on their false positive rates (FPR). It shows exceptional performance for the combined deep learning models, CANET and Hybrid-IDS, which have a better false positive rate of 0.180% and 0.132% [20] [17] respectively. However, classical machine learning models have a slightly higher false positive rate, exceeding 2.147% [24]. Overall, these results highlight the superiority of the combined approach in minimizing false positive rates, making it the preferred choice for detection tasks.

The success of combined deep learning models can be attributed to their unique capabilities in capturing spatial dependencies, translation invariance, hierarchical feature learning and parameter sharing. By leveraging these advanced characteristics, these models are better equipped to identify and interpret complex patterns within network traffic data, leading to highly accurate intrusion detection.

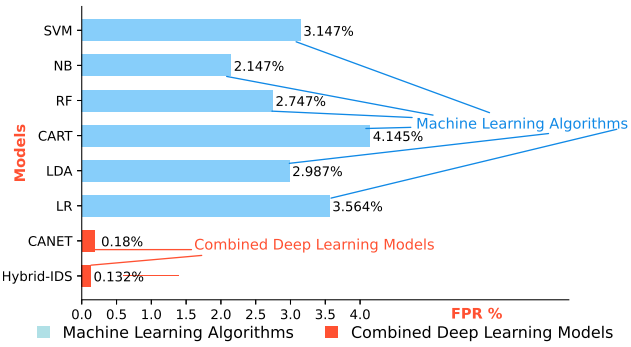

Fig. 12. Comparison based on FPR between Combined DL Models and ML Algorithms Trained with NSL-KDD Dataset

VIII. Future Research Directions

A. Future research proposed for each model

After conducting a study on research papers highlighting the latest trends in network intrusion detection, a trend towards utilizing combined deep learning solutions has been observed. Therefore, in this literature review, we thoroughly examined the most recent and promising solutions. Our comprehensive comparative study, considering various evaluation metrics, was conducted to assess the performance of the combined approach against traditional machine learning and deep learning models.

Table VI summarizes suggestions for future research directions, highlighting both the problems and opportunities for enhancement associated with each stated solution. These major themes have been determined based on our examination of these research papers and will serve as a direction for further investigation.

B. Roadmap to our next research contribution

The project originated from a comprehensive review of recent research conducted between 2021 and 2023, focusing on advancements in intrusion detection. The analysis revealed issues with conventional machine and Deep Learning models, including a false positive rate exceeding 15% and poor feature extraction. Researchers have increasingly turned towards hybrid models combining Deep Learning approaches. However, the rigorous analysis of this hybrid approach in the project unveiled persistent issues. Proficient hybrid models, such as CANET, offer high accuracy and an acceptable false positive rate but suffer from excessively prolonged response times and substantial memory resource consumption. Moreover, their false alarm rate still requires further enhancements. Table VII demonstrates the shortcomings of CANET.

Faced with these challenges, the necessity of creating a new model has emerged, addressing crucial needs: minimizing response time, reducing the false positive rate to the maximum (Figure 13), while preserving overall accuracy and

TABLE VI
SUMMARY AND FUTURE RESEARCH DIRECTIONS FOR THE STUDIED MODELS

Models	Future Research Directions
RideNN-DNFN	- The proposed model has a high false alarm rate. Further research could focus on techniques that reduce the number of false alarms by improving model accuracy and reducing classification errors. - The paper mentions that this detection model has poor reactivity, which leads us to think directly about optimizing the model's temporal performance, by reducing processing times and improving intrusion detection speed. - Data augmentation is an important step in improving model performance, providing high-quality synthetic data that enhances the model's ability to generalize and detect intrusions.
DLNID	- DLNID's performance needs to be validated on real-time data and not on historical data. This would make it possible to check whether the model can be used online to detect intrusions, as is planned for future work. - Strategies to reduce data imbalance should be added, especially for the U2R category.
MLIDS22	- Studying the reasons for the decrease in performance across datasets will help us identify model shortcomings and propose solutions to overcome them.
Hybrid IDS	- It is preferable to use unsupervised classification methods combined with CNNs to make the last step of the algorithm more useful in cases where attack types are not labeled. In the third stage, we propose the use of CAE convolutional auto-encoders, which have convolution layers that learn to reconstruct inputs from themselves, without class labels. - For benchmarking purposes, adapting the GANomaly implementation for 1D data in PyTorch is preferable to using Keras with the TensorFlow backend. - The researchers plan to explore parallelization, and they propose the use of advanced machine learning algorithms to further improve performance in future work.
DOC-IDS	- It is proposed to add additional regularizations, such as L1/L2 regularization, to avoid overfitting and improve model generalization. We could also experiment with different auto-encoder architectures, such as variational auto-encoders, to improve the accuracy of anomaly detection.
DCNNBiLSTM	- Incorporating reinforcement techniques into the model could enable continuous improvement in detection performance by adapting to new forms of attack or learning from previous detection errors. - It would be interesting to evaluate the robustness of the model in situations where the data contains anomalies unrelated to intrusions, to understand how the model reacts to more complex real-life conditions.
CANET	- Adding the attention mechanism to CNNs can increase the computational complexity of the model, which can be reduced by applying model compression and weight quantization methods. This would reduce the number of parameters and operations required while maintaining acceptable performance in terms of intrusion detection. - It's hard to understand why the model focuses on certain parts of the input. Is it possible to understand why the model focuses on specific regions or features? Improving this point will ensure confidence in the decisions made by the model.
GMM-WGAN-IDS	- Using convolutional generative adversarial networks and attention mechanisms to further improve system performance, it will also be important to provide empirical evidence or results to support these claims in future work. - Extend this evaluation to a larger number of datasets to better understand the performance of the proposed method in different contexts.

TABLE VII
CANET MODEL PERFORMANCES

Model	Test Environment	Response Time in μs	FPR in %	Memory usage in KB
CANET	GPU Tesla T4 Driver Version: 525.105.17 CUDA Version: 12.0 RAM: 13.61 Go Disc storage: 78.19 Go Dataset: UNSW-NB15	223	2.66	10 014

adapting the proposed model to environments with limited resources.

IX. CONCLUSION AND FUTURE WORKS

The emergence of cyberattacks in modern times has become a computer flaw that affects all parties involved. The impact of these cyberattacks has become increasingly dangerous, requiring a strategic and rigorous defense. The intrusion detection using a behavioral approach is a rich field in which researchers continue to discover new challenges and suggestions. Deep learning has revolutionized intrusion detection in computer networks over the last few years. Alternatively, it is no longer necessary to use deep learning but rather to optimize detection using new properties such as feature extraction, class imbalance, etc. One of the approaches used nowadays is the combination of deep learning approaches in order to reap the benefits of each model and method. This survey is intended to investigate the detection problem using classical approaches, and then to present the state of the art in new combined solutions, demonstrating the utility of this transition to combination and the aspects added to ensure good feature extraction and class balance.

During this literature review, we compared the performance of combined deep learning solutions and we presented their benefits and their major drawbacks. Then, we suggested improvements to the models under consideration as well as future research directions. This comparison was conducted in a theoretical environment using a variety of research datasets, including NSL-KDD, CIC-IDS2017, CIS-IDS2018, etc. In future work, we propose to analyze the performance of each model in real-world environments. This will allow us to better test the effectiveness and accuracy of the models in

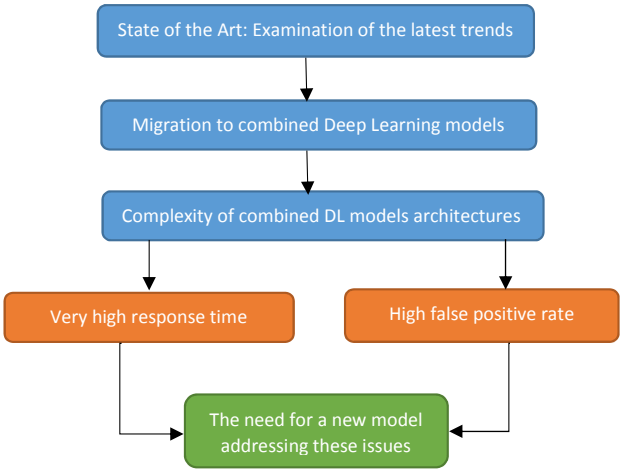

Fig. 13. Identification of the contribution based on the state of the art

detecting real-world intrusions.

REFERENCES

[1] S. Alahmed, Q. Alasad, M. M. Hammood, J.-S. Yuan, and M. Alawad, "Mitigation of black-box attacks on intrusion detection systems-based ml," *Computers*, vol. 11, no. 7, p. 115, 2022. [Online]. Available: https://www.mdpi.com/2073-431X/11/7/115

[2] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804512001944

[3] A. Ajiboye, M. Olumoye, D. Aleburu, A. Olayiwola, D. Olayiwola, and S. Ajose, "Dimensionality reduction for deep learning based intrusion detection systems for iot," *Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2023*, pp. 76–81, 5-7 July 2023.

[4] Y. Zhang, Q. Yang, S. Lambotharan, K. Kyriakopoulos, I. Ghafir, and B. AsSadhan, "Anomaly-based network intrusion detection using svm," in *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*, 2019, pp. 1–6.

[5] P. Negandhi, Y. Trivedi, and R. Mangrulkar, "Intrusion detection system using random forest on the nsl-kdd dataset," in *Emerging Research in Computing, Information, Communication and Applications*. Singapore: Springer Singapore, 2019, pp. 519–531.

[6] S. Waskle, L. Parashar, and U. Singh, "Intrusion detection system using pca with random forest approach," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2020, pp. 803–808.

[7] 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, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/6/916

[8] M. Maithem and G. A. Al-sultany, "Network intrusion detection system using deep neural networks," in *Journal of Physics: Conference Series*, vol. 1804, no. 1, feb 2021, p. 012138. [Online]. Available: https://dx.doi.org/10.1088/1742-6596/1804/1/012138

[9] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Procedia Computer Science*, vol. 185, pp. 239–247, 2021, big Data, IoT, and AI for a Smarter Future. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921011078

[10] H. Jia, J. Liu, M. Zhang, X. He, and W. Sun, "Network intrusion detection based on ie-dbn model," *Computer Communications*, vol. 178, pp. 131–140, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421002760

[11] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional lstm deep learning approach for intrusion detection," *Expert Systems with Applications*, vol. 185, p. 115524, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417421009337

[12] V. S. Kumar and A. Muthukumaravel, "Efficient intrusion detection using deep learning approaches," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10, no. 2s, pp. 180–183, Dec. 2022. [Online]. Available: https://ijisae.org/index.php/IJISAE/article/view/2381

[13] R. Tahri, Y. Balouki, A. Jarrar, and A. Lasbahani, "Intrusion detection system using machine learning algorithms," in *ITM Web Conferences*, vol. 46, 2022, p. 02003. [Online]. Available: https://doi.org/10.1051/itmconf/20224602003

[14] E. S. GSR, M. Azees, C. Rayala Vinodkumar, and G. Parthasarathy, "Hybrid optimization enabled deep learning technique for multi-level intrusion detection," *Advances in Engineering Software*, vol. 173, p. 103197, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0965997822001041

[15] Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, "A deep learning model for network intrusion detection with imbalanced data," *Electronics*, vol. 11, no. 6, p. 898, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/6/898

[16] I. Abdullah Abdulmajeed and I. M. Husien, "Mlids22- ids design by applying hybrid cnn-lstm model on mixed-datasets," *Informatica*, vol. 46, no. 8, 2022.

[17] R. Kale, Z. Lu, K. W. Fok, and V. L. L. Thing, "A hybrid deep learning anomaly detection framework for intrusion detection," in *2022 IEEE 8th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 2022, pp. 137–142.

[18] N. Yoshimura, H. Kuzuno, Y. Shiraishi, and M. Morii, "Doc-ids: A deep learning-based method for feature extraction and anomaly detection in network traffic," *Sensors*, vol. 22, no. 12, p. 4405, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/12/4405

[19] V. Hnamte and J. Hussain, "Dcnnbilstm: An efficient hybrid deep learning-based intrusion detection system," *Telematics and Informatics Reports*, vol. 10, p. 100053, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2772503023000130

[20] K. Ren, S. Yuan, C. Zhang, Y. Shi, and Z. Huang, "Canet: A hierarchical cnn-attention model for network intrusion detection," *Computer Communications*, vol. 205, pp. 170–181, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366423001378

[21] J. Cui, L. Zong, J. Xie, and M. Tang, "A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data," *Applied Intelligence*, vol. 53, no. 1, p. 272–288, apr 2022. [Online]. Available: https://doi.org/10.1007/s10489-022-03361-2

[22] X. Xu, J. Li, Y. Yang, and F. Shen, "Toward effective intrusion detection using log-cosh conditional variational autoencoder," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6187–6196, 2021.

[23] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, "Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities," *IEEE Access*, vol. 10, pp. 112 392–112 415, 2022.

[24] A. K. Balyan, S. Ahuja, U. K. Lilhore, S. K. Sharma, P. Manoharan, A. D. Algarni, H. Elmannai, and K. Raahemifar, "A hybrid intrusion detection model using ega-pso and improved random forest method," *Sensors*, vol. 22, no. 16, p. 5986, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/16/5986

HAMZA KAMAL IDRISSI holds an engineering degree in software engineering from the National School for Computer Science in Morocco. He received his Ph.D. degree in computer security from Mohammed V University in Rabat. In 2020, he joined the Mathematics, Computing, and Networks Department of the INPT (Institut National des Postes et Télécommunications) as an assistant professor in Cybersecurity. His research interests include building intrusion detection systems (IDS), cloud security, and cryptography.