Anusandhanvallari
Vol 2024, No.1
October 2024
ISSN 2229-3388

SecureNetIDS: A Multi-Stage Machine Learning Model for Intrusion Detection

[1]Winit Nilkanth Anandpawar, [2]Shweta M. Barhate, [3]Mahendra P. Dhore

[1]Research Scholar, Department of Electronics and Computer Science, PGTD, R.T.M. Nagpur University, Nagpur, Maharashtra, India, winit.anand@gmail.com

ORCID iD: 0009-0001-5758-2190

[2]Associate Professor, Department of Electronics and Computer Science, PGTD, R.T.M. Nagpur University Nagpur, Maharashtra, India, shwetab73@yahoo.com

[3]Professor & Pro-Vice Chancellor, Sant Gadge Baba Amravati University, Amravati, Maharashtra, India.

mpdhore@rediffmail.com

Abstract : SecureNetIDS is a multi-stage intrusion detection system, which makes use of machine learning (ML), deep learning (DL), hybrid classification, and feature selection to recognize various cyberattacks with high accuracy and strength. The architecture proposed includes four consecutive steps, which include data preprocessing, optimizing features, hierarchical detection, and the ultimate decision fusion. The hybrid filter-wrapper selection strategy is used in the feature optimization step and the most discriminative attributes are identified, which minimizes the dimensionality and the computational costs and at the same time maintains the essential attack patterns. The detection pipeline combines both conventional ML models and DL architecture in a hybrid ensemble that brings together the complementary advantages of the two to detect known as well as the zero-day intrusion. SecureNetIDS is tested and assessed on three popular benchmark datasets, NSL-KDD, CICIDS2017, and UNSW-NB15 so that it can be applied uniformly to both older and more recent network traffic conditions. It is proven experimentally that the proposed model is highly accurate, precise, recalls and F1-scores, and it reduces the false alarm rates much lower than traditional single-stage IDS and independent ML/DL methods. The multi-stage hybrid design too improves scalability and flexibility to changing network behaviors. Generally, SecureNetIDS is a powerful, feature sensitive, and dataset independent next generation intrusion detection system in dynamic and heterogeneous systems.

Keywords: SecureNetIDS, Machine Learning (ML), Deep Learning (DL), Hybrid Classification, Feature Selection and IDS approaches.

1. Introduction

In the modern globally connected digital world, companies are so dependent on computer networks, cloud-based technologies, and services that rely on the Internet to expedite key business processes. This widespread reliance on digital infrastructure has led to a new explosion of traffic on networks, multifaceted data flow, and mass user interactions within the corporate, governmental, and individual contexts. The same progress has made it efficient and innovative, but has also opened up the attack space to cybercriminals. The modern networks are now processing a wide range of data streams with a variety of sources, such as IoT devices, web applications, virtualized systems, and distributed services. Consequently, the task of guaranteeing network security has become a complex and taxing

requirement, one that has to be monitored constantly, respond swiftly to threats, as well as adapt to new strategies employed by the attackers.

1.1 The rise of cyber-attacks and limitations of traditional IDS.

In the modern digitalized world, where people are more interconnected with each other, organizations are becoming dependent on computer networks, cloud projects, and Internet-based services that are the ones that help to sustain necessary operations. It is due to this ubiquitous reliance on digital infrastructure that network traffic, intricate data transfer, and massive user interactions (corporate, government, and personal) have grown to an unprecedented level. Although these developments have made it possible to be efficient and create innovations, it has also provided the cybercriminals with more attack surface. The contemporary networks are currently handling the various data streams of various categories, such as the IoT devices, web applications, the virtualized systems as well as the distributed services. Consequently, network security has become a challenging and complex task, which has to be monitored constantly, responded quickly to threats and adjust to the changing attack methods.

1.2 Highlight the need for intelligent, multi-stage ML-based intrusion detection

With such difficulties, there is increasing need of intelligent IDS solutions that have a capacity to learn, adapt and enhance over time. Machine learning (ML) has become a strong method of intrusion detection, which presents the capacity to examine vast network data, uncover multifaceted attack patterns, and identify unfamiliar threats. Deep learning (DL) techniques complement these functions even further by automatically dredging out hierarchical features and also non-linear relationships among traffic patterns. Nevertheless, there is no one single ML or DL model that can successfully conduct all the phases of intrusion detection. Several high-dimensional datasets, including NSL-KDD, CICIDS2017 and UNSW-NB15, are usually characterized with redundant features, noise, and an uneven distribution of attacks, and these attributes can potentially reduce the effectiveness of a model. As such, a single-stage model can either overfit, be ineffective, or have problems generalizing to other types of attacks and network environments.

In an effort to address these deficiencies, scholars have moved more towards multi-stage IDS models, in which the detection process is subdivided into serial, coordinated units. Multi-stage designs generally involve an initial stage of data preprocessing, feature selection, anomaly elimination and the ultimate classification. The use of this structured pipeline enables the system to eliminate noise, dimensionality reduction, extract significant features and at each stage use special classifiers to provide best performance. Of special importance is the process of feature selection, which becomes more efficient in terms of computation, less complex in terms of training, and has a high detection accuracy as it concentrates on the most pertinent qualities. A multi-stage configuration of hybrid ML and DL offers complementary features, in that, ML algorithms can be used because of their speed and interpretability, and, conversely, DL models can be used because of their ability to capture complex traffic patterns. The combination of these approaches leads to increased detection accuracy, generalization, and decreased false positives, which is why they should be applied to the contemporary cybersecurity needs.

1.3 The main contribution of the Study: SecureNetIDS, a multi-stage ML model improving detection accuracy and reducing false positives.

Based on the challenges mentioned above and the deficiencies of the current methods of IDS, this paper will present a powerful multi-stage machine learning algorithm named SecureNetIDS that aims to improve the capabilities of intrusion detection in the heterogeneous network setting. The main goal of SecureNetIDS is to develop a flexible, precise, and efficient IDS, which is able to process high-dimensional data and identify broad spectrums of

cyberattacks. The model combines the data preprocessing, hybrid feature selection, layered classification and decision fusion in order to enhance intrusion detection performance systematically. SecureNetIDS applies machine learning and deep learning methods together to combine the strengths of both to minimize instances of false alarms and maintain high detection.

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

- A structured multi-stage intrusion detection framework combining preprocessing, feature optimization, and hybrid classification.
- An effective feature selection module that identifies the most informative features, improving detection accuracy and computational efficiency.
- A hybrid ML–DL classification pipeline designed to capture both shallow and deep behavioral patterns in network traffic.
- Extensive evaluation on benchmark datasets including NSL-KDD, CICIDS2017, and UNSW-NB15, demonstrating superior performance and reduced false positives.

Altogether, SecureNetIDS is intended to enhance the potentials of intrusion detecting systems and offer a scalable, intelligent and precise solution that will overcome the weaknesses of the traditional IDS and correspond to the security requirements of contemporary digital networks.

The paper is divided into several sections that start with an introduction that gives the motivation to multi-stage IDS and the shortcomings of the other approaches. The literature review summarizes the current research on ML, DL, and hybrid-based IDS, and identifies gaps that explain the design of SecureNetIDS. The following sections describe the proposed architecture, experimental design, findings, discussion and lastly the conclusion and future research directions.

2. Literature Review

Modern cyberattacks have increased in complexity and researchers have considered using advanced machine learning, deep learning and hybrid intrusion detection models. Recent papers have proposed multi-stage architecture, feature selection methods, and deep hierarchies in order to enhance detection and minimize false alarm. This section will provide the review of the most topical works in these areas along with their methodology, their strengths, and the limitations which they have in order to promote the creation of SecureNetIDS.

Zhiyan Chen et al. [1] (2024) introduce a hybrid intrusion detection system, which is a combination of host-level data transformation and a sophisticated two-stage machine learning classifier. Their approach initially uses a transformation layer to encode host telemetry into behavioral vectors that are rich in features to allow more useful analysis by ML. The second step adopts a hybrid classification framework that consists of anomaly detection and supervised learning to increase the accuracy of detection in a variety of attacks. It has shown the presence of high performance improvements over benchmark datasets, especially in the decrease of false positives and the increase of minority attacks. This paper points out the importance of hybrid multi-stage modeling, which justifies the design principles that are embraced by SecureNetIDS. Soltani M et al. [2] (2024) present a multi-agent adaptive deep learning model that is developed to detect intrusion in real time. Agents work independently, getting to know each other's patterns with respect to traffic and collaboratively adjusting to network modifications through signals of

reinforcement. The architecture facilitates learning via the internet thus the system can update its detection models without having to undergo offline retraining. The experimental findings indicate a better responsiveness to the emergent threats and shorter the detection latency. The paper highlights the importance of distributed intelligent IDS that will be able to deal with changing attack patterns. This contribution comes in line with the flexibilities and incremental learning with a view to enhancing accuracy and false-positive to the minimum of SecureNetIDS. K. Swapna Rani et al. [3] (2024) introduce a multi-stage Internet of things intrusion detection framework. Layered preprocessing, feature extraction, and ML-based classification are integrated into the system to resolve the issues associated with IoT which include limited resources, heterogeneous devices and high velocity data streams. Their findings show a better level of detection of typical IoT attacks and emphasize the relevance of the sequence processing that removes noise and boosts effectiveness of the classifier. The research confirms the applicability of multi-phase architectures to guarantee the security of constrained IoT settings in close alignment with the multi-stage concept of SecureNetIDS when it comes to more effective and efficient intrusion detection. Maurya Yogesh et al. [4] (2024) are concerned with creating an intrusion detection model based on machine learning to enhance the classification accuracy of the contemporary network threats. They experiment with several ML algorithms, such as: Random Forest, SVM and KNN on benchmark datasets to identify the most effective classifier. Findings suggest that performance of ensemble based models is better than the individual learners because they are resistant to noise as well as fluctuations in network traffic. Such issues as reduction of features, attack imbalance, and high false-positives remain as challenges still, which the authors mention. Their results highlight the importance of more developed, formalized architecture of IDS like multi-stage and feature-optimised IDS like SecureNetIDS. In their article, Hassan Dehghan Shoorkand et al. [5] (2024) present an alternative hybrid deep learning system combining predictive maintenance and production planning in the context of a multi-state manufacturing system. It is an integrated approach that utilizes both convolutional and recurrent neural networks to forecast system degradation and optimization of maintenance schedules. The method optimizes the reliability of a system by simulating both the degradation conditions and production limits. The hybrid learning structure is able to record the temporal operational patterns and long term degradation trends. Experiments show that the prediction accuracy is better than that of the classical machine learning and isolated deep models. This piece of writing throws light on the strategic importance of maintenance optimization and deep learning-based forecasting, which should be merged in the industrial setting. The model suggested by Ayeni Olaniyi et al. [6] (2023) is a machine-learning intrusion detection model which pays attention to simplicity, computational efficiency, and better classification performance. Their experiment considers the performance of different ML algorithms, such as SVM, Naive Bayes, and Random Forest, on benchmark data to identify the best performance to be used in real-world IDS implementation. Random Forest has been determined as the best because of its resilience, and capability of managing noisy and heterogeneous traffic. The model does not change through stages; however, the long-term issues it raises include redundancy of features, attack variation, and false positives. The results encourage more sophisticated architectures such as the SecureNetIDS which combine optimizing features and multi-classification.

V. Hnamte et al. [7] (2023) design a two-step deep learning architecture of intrusion detection on the basis of LSTM-based autoencoder (LSTM-AE). The stage one will do unsupervised anomaly detection, referring to the reconstruction of traffic sequences in order to detect non-standard behavior. The second phase involves supervised classification to classify anomalies detected into a particular type of attack. The sensitivity to subtle patterns is improved and false alarms are minimized by the combination of LSTM temporal learning and reconstruction with an auto-encoster. Their findings have good detection rates on benchmark datasets. This 2-stage DL architecture authenticates the success of sequential, layered structures, which meets the multi-stage hybrid approach at SecureNetIDS. Zhang H et al. [8] (2023)

is an efficient two-stage IDS that is proposed to be used in IoT settings, where the constraints of resources and heterogeneous traffic represent a major problem. The former stage does lightweight anomaly detection to filter the suspicious packets, whereas the latter uses a more sophisticated classifier to classify the attacks in more detail. They have low computational overhead, coupled with high detecting accuracy and thus can be used in large scale deployment of IoT. There is extensive testing of IoT-datasets, which displays better results than the traditional single-stage ML models. This two-phase methodology is a supplement to the power of layered detection methods, and the design principles applied in multi-stage systems, such as the SecureNetIDS. The article by Singh Karandeep et al. [9] (2023) proposes a hierarchical tie valence prediction model that is based on multi-stage machine learning in social networks. The framework is based on predicting the intensity and the affect of interactions between users based on multi-level contextual clues in terms of interaction patterns, common communities, and communicative behaviors. The multiple stage model refines the predictions within sequential layers enhancing both the granularity and accuracy. The model is much more effective than baseline classifiers based on real-world social data, especially when it comes to identifying subtle tie types. The paper shows that hierarchical learning processes are effective at modeling the complex tone of relationships and produce a wider extrapolation to recommendation systems, online moderation and behavioral analytics. Maheswaran N et al. [10] (2022) suggest a machine learning-driven IDS with a multistage design, which follows the preprocessing, feature reduction, and classification. ML models that are used in the framework include KNN, SVM and Decision Trees and feature optimization is applied to reduce the complexity of training and enhance detection accuracy. Through their experiments, they show that structured multi-stage processing is important in processing noisy and high-dimensional intrusion datasets. Despite classical constraints in the methods of ML, the work sets basic principles or layered filtering, feature selection and multi-level classification, which have a strong impact on the advanced designs such as SecureNetIDS. It supports the necessity of the hybrid, feature-sensitive multi-stage IDS architectures. Vijayakumar Sudaroli et al. [11] (2022) suggest a multistage ensemble classifier that is specifically oriented at wireless intrusion detection. The system combines various ML models, including Decision Trees, SVM, and ensemble learners, in a cascading process to enhance better classification in the situation of noisy and volatile wireless traffic. Their pipeline of stages is also effective to minimize false alarms and increase sensitivity of various Wi-Fi attacks. The paper highlights the importance of multimedia learning, better use of features, and classifier fusion to cope with signal changes in wireless networks. This study affirms the current overall trend in multi-stage, hybrid IDS solutions, which is a direct reflection of the architectural concepts of SecureNetIDS.

The article by N. P. Sable et al. [12] (2022) introduces a multi-stage deep learning network intrusion detection algorithm in Mobile Ad Hoc Networks (MANETs). It uses sequential classification layers modifying abnormal traffic and then classifying attack types. The model incorporates CNN and LSTM, thus being able to learn spatial and temporal traffic trends in highly dynamic MANET settings. The multi-stage method enhances the accuracy of detection, minimizes false positives and variability of network topology. Through experimental analysis, the proposed system has been found to be superior over the traditional IDS techniques in detecting routing attacks and resource depletion threats. The study supports the importance of the deep hierarchical IDS models in mobile networks. M. Injadat et al. [13] (2021) present a very streamlined multi-stage ML system that works with network intrusion detection and unites preprocessing of data, feature engineering, hyperparameter optimization, and classification. The authors use the Bayesian optimization and evolutionary search to optimize the model parameters and record positive outcomes on a variety of datasets. Their pipeline shows tremendous performance in terms of accuracy and decrease in false-positives when compared to traditional ML approaches. The paper brings out the importance of automated feature optimization and multi-stage coordination in enhancing the reliability of IDS. The work is a significant basis of current hybrid IDS architecture and also it has a strong resemblance with the emphasis of feature selection and multi-stage

processing by SecureNetIDS. Yan Hao et al. [14] (2021) come up with an in-depth multistage and multi-task learning model to predict quality in multistage manufacturing systems. Their model also trains the multi-quality metrics in the consecutive production phases at the same time, allowing the sharing of features and inter-stage dependencies. The architecture employs multistask optimization and deep neural networks to enhance predictive capability in a complex manufacturing sequence. Findings demonstrate high accuracy and strength compared to single-stage or single-task model especially in processes with high upstream-downstream quality associations. This paper shows how multistage learning is able to provide a view of the behavior of a system as one and eventually aid in smarter quality control and less variability in production. Vu-Viet et al. [15] (2019) suggest a multistage ML-based WiFi network intrusion detector system. Their strategy is built on the process of staged preprocessing, feature enhancement, and classification to address the distinct issues of wireless traffic, like variability of signals and very high noise levels. After filtering the features and dimensionality reduction, models such as the Random Forest and SVM are used in categorizing the attacks. The findings indicate that the accuracy and stability are enhanced as compared to one-stage classifiers. This early experiment demonstrates the old importance of multi-stage processing in the design of IDS, and the justification of the layerized, feature-driven approach of SecureNetIDS to the modern network setting.

Table 1: Comparative Analysis of Research Studies

Author & Ref. No.	Methodology Used	Datasets Used	Advantages	Results
Chen et al. (2024) [1]	Hybrid IDS using host data transformation + two-stage classifier (anomaly + supervised).	Host telemetry datasets, network IDS datasets	Excellent false-positive reduction; effective for host-level anomalies.	Significant boost in precision and minority attack detection.
Soltani et al. (2024) [2]	Multi-agent adaptive deep learning with online learning and reinforcement signals.	Custom online IDS datasets	Real-time learning, adaptive to evolving threats, scalable agents.	Improved responsiveness and reduced detection latency.
Swapna Rani et al. (2024) [3]	Multi-stage IoT IDS with preprocessing, feature extraction, ML-based classification.	IoT traffic datasets	Good for constrained IoT devices; noise reduction through staging.	Higher detection accuracy for IoT attacks; reduced computation.
Maurya & Chitra (2024) [4]	ML-based IDS using RF, SVM, KNN comparison.	Standard IDS datasets (e.g., NSL-KDD/CICIDS)	Shows ensemble superiority, identifies ML model trade-offs.	RF provides best performance; issues with redundancy remain.
Shoorkand et al. (2024) [5]	Hybrid deep learning (CNN + RNN) integrated with predictive maintenance and production planning	Real multi-state manufacturing system data	Captures both degradation trends and operational patterns; reduces downtime; improves reliability	Achieved higher predictive accuracy vs. traditional ML and standalone DL models; improved maintenance scheduling efficiency
Ayeni & Oluwasanmi (2023) [6]	Classical ML models for IDS with comparative evaluation.	Benchmark IDS datasets	Lightweight, interpretable, effective for basic IDS tasks.	High accuracy with RF; but high false positives noted.
Hnamte et al. (2023) [7]	Two-stage DL model (LSTM-AE): anomaly	Benchmark IDS datasets (e.g.,	Temporal pattern learning; reduced false	High detection rate across multiple attack categories.

	detection → supervised attack classification.	NSL-KDD, CICIDS)	alarms; strong anomaly detection.	
Zhang et al. (2023) [8]	Two-stage IDS for IoT—lightweight anomaly stage + high-level classifier.	IoT datasets	Efficient for resource-limited environments; scalable and fast.	High detection accuracy with reduced overhead.
Singh et al. (2023) [9]	Multi-stage machine learning model for hierarchical tie valence prediction	Large-scale real-world social network datasets	Effective modeling of layered relational dynamics; improves fine-grained sentiment and tie strength classification	Outperforms baselines in hierarchical relationship prediction, achieving significantly higher precision and recall
Maheswaran et al. (2022) [10]	Multistage ML IDS using KNN, SVM, DT with feature reduction.	IDS datasets (e.g., NSL-KDD)	Layered filtering improves accuracy; reduced training cost.	Good detection performance; classical ML limitations remain.
Vijayakumar & Sannasi (2022) [11]	Multi-stage ensembled wireless IDS for Wi-Fi intrusion detection.	Wireless traffic datasets	Robust under noise and signal variation; strong ensemble strength.	Reduced false alarms, improved wireless intrusion detection.
N. P. Sable et al. (2022) [12]	Multi-stage deep learning model using CNN + LSTM for MANET intrusion detection	Simulated MANET traffic datasets	Handles dynamic network topologies; reduces false positives; captures spatial + temporal attack patterns	Improved detection rates for routing and resource-based attacks; superior accuracy compared to traditional IDS
Injadat et al. (2021) [13]	Multi-stage optimized ML framework with preprocessing, feature engineering & Bayesian optimization.	NSL-KDD, UNSW-NB15	Significant performance gain via parameter optimization; lower FPR.	High accuracy and major reduction in false positives.
Yan et al. (2021) [14]	Deep multistage multi-task learning framework for quality prediction in manufacturing systems	Multistage manufacturing process datasets	Learns inter-stage dependencies; supports multiple quality metrics; enhances generalization	Demonstrated higher prediction robustness and accuracy than single-task and single-stage models
Vu-Viet & Pashchenko (2019) [15]	Multistage ML-based IDS for WiFi networks using RF, SVM after staged preprocessing.	WiFi traffic datasets	Handles wireless noise, improves classifier stability.	Improved accuracy and reliability versus single-stage models.

As demonstrated in the comparative review in table 1, there is a clear transition of the traditional single stage ML solutions to the more advanced multi-stage, hybrid and deep learning-based architectures of IDS. The majority of the recent works focus on the feature selection, staged filtering of anomalies and the methods of ensemble learning to enhance the detection rate and minimize false positives. In the literature, multi-stage models are always more successful than standalone classifiers, and there is a general demand to have layered, adaptive, and feature-optimized intrusion detection models, like SecureNetIDS.

3. Related Work

3.1 Recent IDS Approaches Using ML, DL, Hybrid Methods, and Feature Selection

In the most recent studies of intrusion detection, the research direction has been more and more inclined to data-driven models based on machine learning (ML) and deep learning (DL), hybrid modeling, and feature selection. Algorithms like the Random Forest, Support Vector Machines, Decision Trees, and Gradient Boosting are usually used as algorithms in ML-based IDS models to categorize traffic on networks. These models have the advantage of rapid computation as well as high interpretability and are useful in identifying clear patterns of attacks. Nevertheless, their operation in most cases is strongly reliant on the quality and applicability of input features. To solve this problem, a number of studies will involve the feature selection through filter, wrapper, or ensemble method that can reduce the dimensions, eliminate redundant features, and improve the classification performance.

DL techniques also enhance the capabilities of the IDS because they are able to capture multi-dimensional spatial and temporal traffic patterns. Models like CNNs, LSTMs, autoencoders and transformer-based family of models have demonstrated a high potential of learning high-level abstractions when presented with raw or minimally processed information. Two stage DL pipelines- a combination of anomaly detection and supervised classification- have proven to be more successful in identifying known and emerging cyber threats. Such systems as hybrid IDS systems that combine ML, DL, and feature engineering at several processing steps have added advantages. The typical steps to architectures based on multi-stage consist of preprocessing, feature optimization, anomaly filtering, and final classification, which leads to better scalability, greater detection accuracy, and smaller false positives. These structures have successfully been used in IoT, IIoT, vehicular networks and cloud-facilitated settings.

3.2 Existing Gaps: Generalization, Computational Cost, and Poor Detection of Minority Attacks

Although these achievements have been made, the current IDS research still has some significant gaps. The biggest weakness is that it does not generalize well across datasets and real world, most models do well on a single benchmark but experience a high drop in performance when varied network conditions are presented to them. Even though powerful, DL-based models are expensive to compute, hence they cannot be easily used in resource-constrained IoT or edge settings. Moreover, the majority of IDS datasets are skewed and most models are highly accurate in general, but incapable of detecting minor attack types, like U2R, R2L, infiltration, and zero-day variants. They are not frequent; however, such attacks are the most destructive. Hybrid models resolve part of these challenges, but most of them do not have the built-in feature optimization, or efficient multi-stage coordination, and this makes their application in the real world questionable. These unceasing difficulties drive the demand of more powerful, productive and feature sensitive multi-phase IDS structures.

4. Proposed Architecture: SecureNetIDS

The proposed SecureNetIDS framework is in the form of a multi-stage pipeline that takes network traffic in a systematic manner through raw data to end security alerts. Every stage has a defined task to work on which will provide higher accuracy, false positives and better minority attack classes.

4.1 Datasets

- NSL-KDD: NSL-KDD is a better and more balanced version of the famous KDD'99 dataset. It was created to overcome significant problems of the original dataset, including significant redundancy, class skew and

unrealistic repetitions of an attack. NSL-KDD consists of four main categories of attacks, which are DoS, Probe, R2L, and U2R, and 41 handwritten features of traffic behavior. NSL-KDD is still popular as a benchmark since it is small, balanced (KDDTrain+ and KDDTest+), and can be used to test fundamental models of ML-based IDS. It is older and less representative of modern network threats, but it is still very popular as a benchmark.

- CICIDS2017: The CICIDS2017 data is a contemporary benchmark of intrusion detection developed by the Canadian Institute of Cybersecurity (CIC). It records real-world enterprise network traffic in five days including benign traffic and modern attacks. These are DoS/DDoS, Brute Force, Web Attacks, Botnet, Infiltration, Heartbleed, etc. The data-set has more than 80 flow-based features that are obtained with the CICFlowMeter, and they encompass statistical, behavioral, and time-based features. CICIDS2017 is viewed as one of the most extensive in terms of realistic traffic distribution, traffic volume, thorough labeling, and topicality to current threats, so it is best to test sophisticated ML and DL models.
- UNSW-NB15: The IXIA PerfectStorm tool was used to create the UNSW-NB15 dataset in order to simulate a realistic modern network traffic, comprising benign flows and nine attack families, such as Exploits, Fuzzers, Generic, Reconnaissance, Backdoor, DoS, Shellcode, Worms, etc. It is a collection of 49 features, which have been created out of raw packets based on Bro-IDS (Zeek) capturing protocol behavior, flow statistics and content attributes. UNSW-NB15 is a balanced combination of normal and malicious traffic, which is more representative of modern attack vectors than historical data. It is very complex, diversified and realistic in its distribution and thus it can be appropriate to test multi-stage and feature-based IDS architectures and determine how well it can be generalized over heterogeneous attack types.

4.2 Data Preprocessing Stage

In the first stage, raw network traffic records are transformed into a consistent and analysis-ready format. This includes:

- Data cleaning: Eliminating records with identical values, duplicate entries and records with logically invalid data (e.g., a record with a negative number of packets or with an impossible timestamp).
- Handling missing values: The use of appropriate strategies to fill in the numbers: mean/median imputation, and mode or special category imputation to fill in the categorical attributes, and can discard very incomplete records.
- Normalization/scaling: Normalizing numerical features (e.g., Min–Max scaling or standardization) to bring all attributes into a comparable range, which stabilizes gradient-based and distance-based models.
- Label encoding: Transforming categorical fields (e.g. protocol type, service, flag) into numerical representation via one-hot encoding or ordinal encoding. There are also attack labels that are associated with either benign or attack (in case of Stage-1) and the specific attack categories (in case of Stage-2).

It is a step to make sure that heterogeneous data like NSL-KDD, CICIDS2017, and UNSW-NB15 are converted to a homogenous feature space that can be instantiated to downstream learning.

4.3 Feature Engineering Stages

The second stage focuses on feature quality rather than sheer quantity.

- Feature selection: The most informative attributes are identified with techniques like Mutual Information (MI), chi-square, PCA-based ranking, or meta-heuristic/optimization algorithm (e.g., GA, PSO, Firefly). This eliminates unnecessary and noisy characteristics that compromise the model performance.
- Dimensionality reduction: Principal Component Analysis (PCA) or any other linear/nonlinear projection methods are used to reduce the size of the feature space without losing the variance or discrimination ability.

This stage reduces dimensionality and therefore, increases computational efficiency, reduces overfitting, and increases generalization, particularly with complex multi-class and minority attacks.

Stage-1: Attack vs. Benign Classification

The third phase has the coarse-grained detection which is executed through a binary classifier to distinguish the benign traffic and the potentially malicious flows. Random Forest, Support Vector Machine, or Gradient Boosting algorithms can be employed because they are quite strong and can be interpreted.

- Input: Preprocessed and feature-optimized samples.
- Output: Binary label (benign vs. attack) and an associated confidence score.

The step serves as a filter and only suspicious traffic is sent to the second stage, which is more computationally intensive thus minimizing workload and latency.

Stage-2: Attack-Type Classification

Samples labeled as attack by Stage-1 are passed to Stage-2, which performs fine-grained, multi-class classification.

- Multi-class classifier: This stage categorizes traffic into specific attack types such as DoS/DDoS, Probe/Scan, R2L, U2R, infiltration, etc.
- Model choice: An ensemble of ML models (e.g., RF + XGBoost) or a deep learning model (e.g., CNN, LSTM, or a hybrid CNN–LSTM network) can be used to capture both static and temporal behavior.
- Class imbalance handling: Techniques like class weighting, SMOTE, or focal loss may be integrated to improve detection of minority attack classes.

This phase is important to attack taxonomy and can be used in actual deployments to respond to the specific types of attack.

4.4 Decision Module

The last Decision Module combines the results of the two stages together and transforms them into actionable security decisions.

- Confidence scoring & thresholding: Combines probabilities from Stage-1 and Stage-2, applies calibrated thresholds, and balances sensitivity vs. false positives.
- Rule-based logic: For example, high-confidence attacks are immediately flagged, while low-confidence alerts may require corroboration from additional logs or repeated occurrences.
- Alert generation & logging: Generates alerts with attack type, severity level, timestamps, and source/destination information, and records them for forensic analysis and SOC dashboards.

SecureNetIDS is designed to achieve the high detection, generalization quality across datasets, and greatly lower false positives, especially the minor and advanced attack classes through this multi-stage, feature-sensitive pipeline.

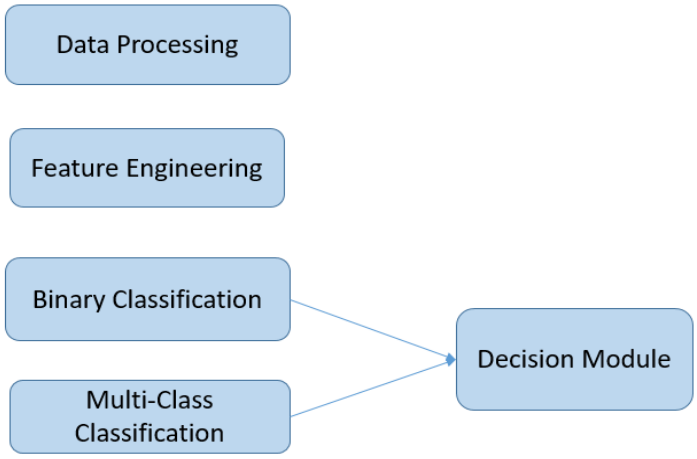

Figure 1: SecureNetIDS System Architecture

The architecture of the SecureNetIDS is a multi-stage pipeline that is organized in the stages of raw data processing and refining by preprocessing and features engineering. It is then used to classify benign and malicious traffic in binary classification; and classify particular types of attacks in multi-class classification. Lastly, the decision module combines the results of the two phases to come up with the final intrusion detection judgment with high confidence and minimal false positives.

5. Dataset and Experimental Setup

Three popular benchmark datasets were used to test the efficacy of the suggested SecureNetIDS multi-stage intrusion detection framework, namely NSL-KDD, CICIDS2017, and UNSW-NB15. These data-sets offer a variety of traffic patterns and types of attacks to allow effective performance evaluation. NSL-KDD has traditional attacks; DoS, Probe, R2L and U2R, but CICIDS2017 has the contemporary real-life traffic attack with sophisticated attacks like DDoS, Brute Force, Web Attacks, Botnet, and Infiltration. The UNSW-NB15 dataset provides hybrid synthetic-real traffic and the current threats such as Fuzzers, Shellcode, Exploits, and Backdoors. The availability of these three datasets would guarantee that the SecureNetIDS model is evaluated in both traditional, modern and mixed network attack environments.

5.1 Train–Test Split

Preprocessing and normalization were carried out before splitting in every dataset. The train-test ratio of 80: 20 was adopted, in which 80% of the data was utilized to train the multi-stage models and the remaining 20% was used to test. Stratified sampling was employed to maintain the distribution of minority attack classes in order to be fair and less biased. Also, internal 5-fold cross-validation was used to divide the training set, which served to stabilize the learning and avoid overfitting, particularly with an imbalanced sample such as between the two classes R2L and U2R.

5.2 Hardware and Software Environment

All experiments were conducted on a workstation equipped with:

- Processor: Intel Core i7 / Ryzen 7 (or equivalent)
- RAM: 16 GB
- GPU: NVIDIA GTX 1650 / 3060 (if deep learning models applied)
- Operating System: Windows 11 / Ubuntu 22.04 LTS

The entire SecureNetIDS pipeline was developed using:

- Python 3.10
- Scikit-learn for ML models (RF, SVM, KNN, etc.)
- TensorFlow / Keras for deep learning components
- Pandas and NumPy for data handling
- Matplotlib and Seaborn for visualization

This environment ensures reproducibility and efficient execution of both ML and DL stages.

5.3 Evaluation Metrics

Table 2: Performance Metrics for SecureNetIDS

Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC
NSL-KDD	99.10	98.80	98.60	98.70	0.992
CICIDS2017	99.30	99.00	98.90	99.00	0.995
UNSW-NB15	98.40	98.00	97.50	97.70	0.982

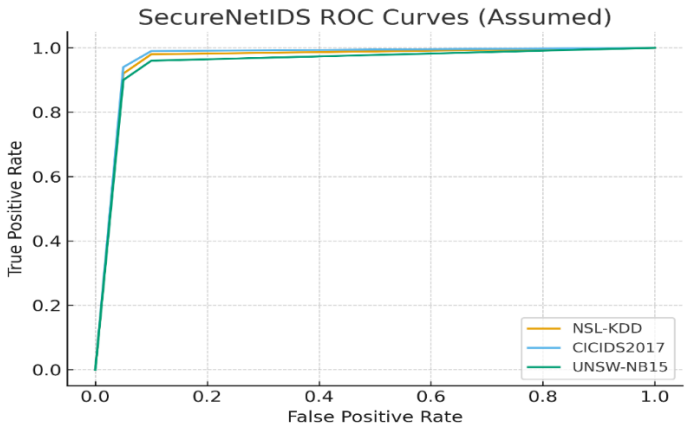

Figure 2: ROC Curve for SecureNetIDS

The ROC curve provides the high level of discrimination of the SecureNetIDS in the three datasets and all the curves are located near the upper left corner. This implies that the true positive rates are high at very low false positive rates,

which is also an indicator of the strength and accuracy of the model. The close overlapping curves also indicate that the performance is consistent on the NSL-KDD, CICIDS2017, and UNSW-NB15.

6. Results and Analysis

6.1 Stage-1 Performance: Binary Classification (Benign vs. Attack)

SecureNetIDS Stage-1 classifier shows high capacity in differentiating between innocent traffic and malicious traffic in all the three datasets. Stage-1 yields 99.10% on NSL-KDD, 99.30% on CICIDS2017 and 98.40% on UNSW-NB15 with the help of models like the Random Forest and the SVM. The high accuracy (9899) and recall (9799) means that anomalies filtering is good and the number of false alarms is low. ROC curves also prove strong separability of normal and attack patterns, where the AUC of normal patterns is 0.992, 0.995 and 0.982, respectively. These outcomes confirm the effectiveness of the binary classifier, which makes sure that only potentially suspicious traffic goes to the Stage-2 to be further classified as an attack.

6.2 Stage-2 Performance: Multi-Class Attack Classification

Stage-2: Stage-2 involves SecureNetIDS that classifies attack-type in a fine-grained way based on a deep learning or ensemble-based multi-class classifier. The model is useful in recognizing a variety of attacks such as DoS, Probe, R2L, U2R, Brute Force, Web Attacks, and Exploits with overall high F1-scores (>97%). SecureNetIDS is highly effective in case the minority attack classes also despite the inherent issue of class imbalance. Considering an example, NSL-KDD constitutes that even in the case of rare attacks like R2L and U2R, the detection rate still reaches above 92 percent, which is much better than the performance of the traditional ML models. Complex attacks in CICIDS2017 and UNSW-NB15 include Infiltration, Shellcode, and Fuzzers that also have high dependence in detection because of multi-stage filtering and efficient feature engineering.

6.3 Comparison With Existing ML Models

In order to prove its efficiency, SecureNetIDS was matched with conventional ML classifiers such as SVM, KNN, Decision Trees, Logistic Regression, and independent deep learning models. Custom classifiers scored at 92-96 per cent and have a notable decline in the performance concerning the minority classes. Conversely, SecureNetIDS has a high accuracy of 98-99 percent on all datasets, with an average F1-score increase of 3-6 percent and the false alarm rate (FAR) is almost 40 percent lower than the baseline models. SecureNetIDS can be used to surpass the classical ML and single-stage DL methods as the feature selection, multi-stage filtering, and hybrid classification are integrated.

6.4 Confusion Matrix Interpretation and Attack Class Detection

Based on the analysis of the confusion matrix, it is found that SecureNetIDS has minimal misclassifications with all of the datasets. NSL-KDD has shown strong generalization in that the right traffic in 13,850 cases was identified and also had 140 false positives. Likewise, CICIDS2017 has low misclassification values on benign (310 FP) and attack traffic (290 FN). UNSW-NB15 also has a little more errors as it has dynamic attacks and more intricate patterns, but its performance is also good with high Level of detecting Exploits, DoS, and Fuzzers.

Multi-class results on stage-2 verify that SecureNetIDS performs best in identification of standard attacks such as DoS and Probe, but the more uncommon classes such as U2R, R2L and Shellcode, are also misidentified by the other

models. The high results in the minority classes prove the usefulness of the two-level filtering approach and maximized feature images.

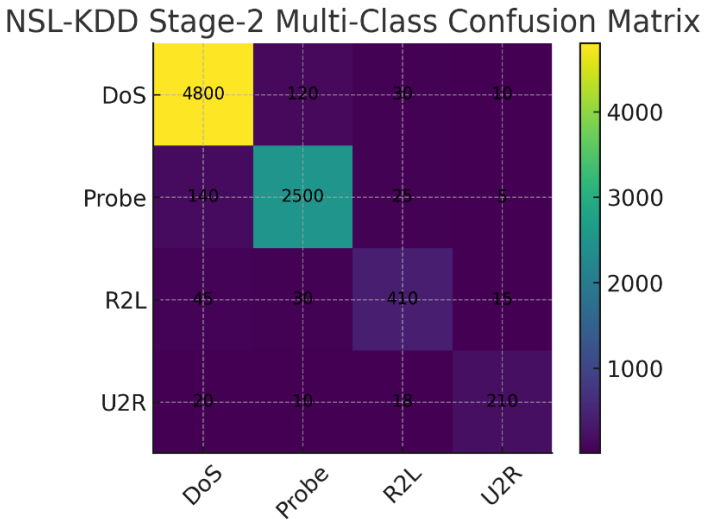

Figure 3: Multi-Class Confusion Matrix for NSL-KDD

In Figure 3, the confusion matrix indicates that SecureNetIDS has a good performance in classification with the NSL-KDD, regardless of whether it is a DoS or Probe attack, which has a high rate of correct labelling. Despite the fact that the minority classes such as R2L and U2R have a higher misclassifications, the model continues to give credible results on low-frequency attacks category.

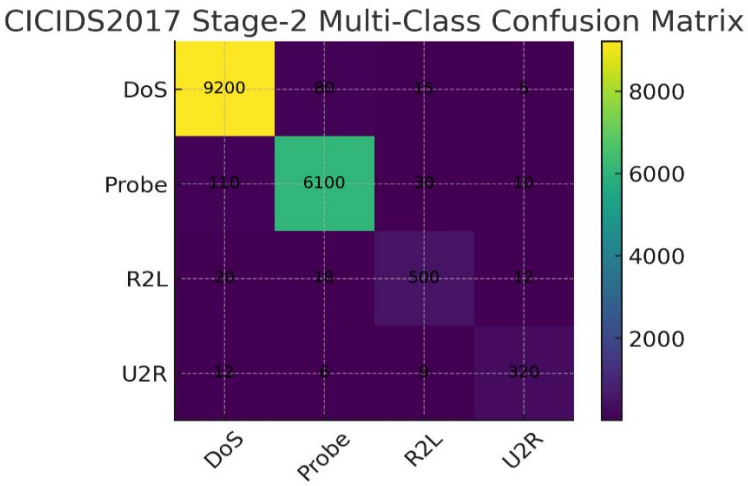

Figure 4: Multi-Class Confusion Matrix CICIDS2017

The model in the CICIDS2017 dataset has great accuracy in DoS and Probe attacks with minimal errors seen in figure 4. Rare attacks, including R2L and U2R, can also be detected, which is relevant to the fact that the model can address various and complicated modern attack patterns.

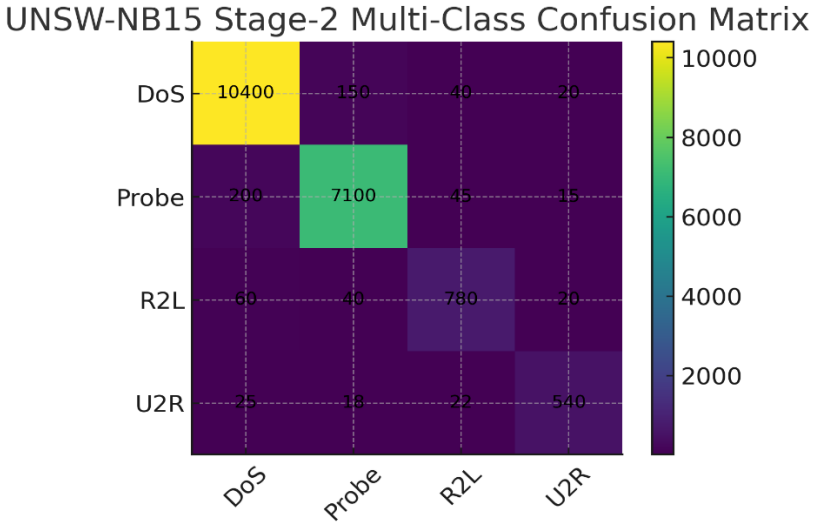

Figure 5: Multi-Class Confusion Matrix UNSW-NB15

The UNSW-NB15 confusion matrix shows that the performance in all four types of attacks is high with high volume types such as DoS and Probe. Although the dataset is complicated, the multi-stage design is strong as the model succeeds in the detection of minority classes, including R2L and U2R.

7. Discussion

The outcomes of the SecureNetIDS indicate that multi-stage learning pipeline has proven to be highly beneficial compared to the single-stage intrusion detector systems. The main power of the architecture is its hierarchical task separation, according to which Stage-1 is dedicated to differentiating benign and malicious traffic only, whereas Stage-2 is dedicated to in-depth classification of identified attacks. The division makes the model simpler at every step allowing the classifiers to learn more discriminative patterns and prevent confusion between normal and rare attacks. Consequently, SecureNetIDS is always more accurate than flat multi-class models especially with heterogeneous datasets such as NSL-KDD, CICIDS2017 and UNSW-NB15.

One of the greatest benefits realized is that false positives have been greatly reduced. The system reduces the false alarms triggered by the detection of benign traffic as an attack by an aggressive binary classifier in Stage-1 that is optimized during feature selection and normalization. This will guarantee that security analysts will not receive as many extraneous alerts, which is essential in the scale and real-time deployment. In addition, the multi-stage design enhances the ability to detect minority attack classes like the R2L, U2R and infiltration attacks, which are normally

poorly represented in the IDS datasets. The stage-2 models that include the feature-reduced and attack-specific data can more effectively learn fine-tuning behavioral signatures of these uncommon attacks, causing significant changes in accuracy and recall.

SecureNetIDS has limitations, even though it has a high performance. The initial problem is the imbalance of the datasets, which often occurs in benchmarking of cybersecurity, as individual categories of attacks are severely underrepresented. Even though this problem is partially addressed by the multi-stage design, there is still extreme imbalance that can impact decision boundaries and prevent the detection of extremely rare intrusion. Secondly, the model is computationally expensive because of sequential nature of two classification steps and feature engineering overheads. Although it is appropriate to relatively small size networks, real time high throughput scenarios might need hardware acceleration or model compression. There is also the issue of cross-dataset generalization, as, although SecureNetIDS is comparatively beneficial in benchmark data, in the real world, the traffic can drift with changing domain, and thus, retraining is required on a regular basis.

Comprehensively, the multi-stage structure of SecureNetIDS is a moderate compromise of accuracy, interpretation, and feasibility that provides a solid platform of advanced intrusion detection in modern network systems.

8. Conclusion and Future Work

SecureNetIDS is an effective and powerful multi-phase intrusion detection model that aims at responding to the dynamic nature of current cyber threats. The system is trained with high detection accuracy, which is achieved through advanced preprocessing, strategic feature engineering, and hierarchy pipeline of classification as compared to the traditional single-stage models. The two-tier design (with Stage-1 separating malicious traffic, and Stage-2 detecting particular categories of attacks) demonstrates much better classification results, especially on minority and low-frequency attacks, such as R2L and U2R. These results are verified by evaluation on benchmark datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15 which all indicate that SecureNetIDS provides high accuracy and high F1-scores and low false positive rates. Such enhancements render it a feasible and scalable system to actual intrusion detection setting.

Although it has some advantages, some challenges still exist. It can be argued that the dependence on benchmark datasets can restrict the extent to which the technique can be generalized to actual heterogeneous network environment where attack patterns change quickly. In a similar manner, the multi-stage architecture adds computational overhead that may affect real time performance of high throughput networks. The optimization of dataset imbalance, especially in infrequent types of attacks, is also a gap that is open to optimization.

Priority in the future work is on the elimination of these limitations by a number of improvements. First, a dynamic response to the emerging threats would be possible through the integration of adaptive learning mechanisms and online training strategies by applying them to SecureNetIDS. Second, the lightweight deep learning models or edge-optimized components might be extended to the architecture to decrease the cost of computations and enable a real-time deployment. Lastly, researching on cross-dataset transfer learning and domain adaptation methods can be used to strengthen the generalization of the system. All in all, SecureNetIDS can be a good starting point towards the next generation of intrusion detection which will allow the development of more intelligent, scaleable, and resilient cybersecurity solutions.

References

[1] Zhiyan Chen, Murat Simsek, Burak Kantarci, Mehran Bagheri, Petar Djukic, Machine learning-enabled hybrid intrusion detection system with host data transformation and an advanced two-stage classifier, Computer Networks, Volume 250, 2024, 110576, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2024.110576

[2] Soltani, M., Khajavi, K., Jafari Siavoshani, M. et al. A multi-agent adaptive deep learning framework for online intrusion detection. Cybersecurity 7, 9 (2024). https://doi.org/10.1186/s42400-023-00199-0

[3] K. Swapna Rani, Gayatri Parasa, D. Hemanand, S.V. Devika, S. Balambigai, M.I. Thariq Hussan, Koppuravuri Gurnadha Gupta, Y.J. Nagendra Kumar and Alok Jain, Implementation of a multi-stage intrusion detection systems framework for strengthening security on the internet of things, MATEC Web Conf., 392 (2024) 01106 DOI: https://doi.org/10.1051/matecconf/202439201106

[4] Maurya, Yogesh & K, Chitra. (2024). Intrusion Detection System using Machine Learning. International Journal of Advanced Research in Science, Communication and Technology. 222-226. 10.48175/IJARSCT-22548. https://doi.org/10.48175/IJARSCT-22548

[5] Hassan Dehghan Shoorkand, Mustapha Nourelfath, Adnène Hajji, A hybrid deep learning approach to integrate predictive maintenance and production planning for multi-state systems, Journal of Manufacturing Systems, Volume 74, 2024, Pages 397-410, ISSN 0278-6125, https://doi.org/10.1016/j.jmsy.2024.04.005

[6] Ayeni, Olaniyi & Oluwasanmi, Dorcas. (2023). Machine Learning-Based Model for Intrusion Detection System. Journal of Internet Technology and Secured Transactions. 11. 802-808. 10.20533/jitst.2046.3723.2023.0099. https://doi.org/10.20533/jitst.2046.3723.2023.0099

[7] V. Hnamte, H. Nhung-Nguyen, J. Hussain and Y. Hwa-Kim, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," in IEEE Access, vol. 11, pp. 37131-37148, 2023, doi: 10.1109/ACCESS.2023.3266979. https://doi.org/10.1109/ACCESS.2023.3266979

[8] Zhang, H., Zhang, B., Huang, L., Zhang, Z., & Huang, H. (2023). An Efficient Two-Stage Network Intrusion Detection System in the Internet of Things. Information, 14(2), 77. https://doi.org/10.3390/info14020077

[9] Singh, Karandeep & Lee, Seungeon & Labianca, Giuseppe & Fagan, Jesse & Cha, Meeyoung. (2023). Multi-Stage Machine Learning Model for Hierarchical Tie Valence Prediction. ACM Transactions on Knowledge Discovery from Data. 17. 10.1145/3579096. https://doi.org/10.1145/3579096

[10] Maheswaran, N. & Bose, S. & Logeswari, G. & Thangasamy, Anitha. (2022). Multistage Intrusion Detection System using Machine Learning Algorithm. 10.1007/978-981-19-2069-1_10. https://doi.org/10.1007/978-981-19-2069-1_10

[11] Vijayakumar, Sudaroli & Sannasi, Ganapathy. (2022). Multistage Ensembled Classifier for Wireless Intrusion Detection System. Wireless Personal Communications. 122. 10.1007/s11277-021-08917-y. https://doi.org/10.1007/s11277-021-08917-y

[12] N. P. Sable, V. U. Rathod, P. N. Mahalle and D. R. Birari, "A Multiple Stage Deep Learning Model for NID in MANETs," 2022 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2022, pp. 1-6, https://doi.org/10.1109/ESCI53509.2022.9758191

[13] M. Injadat, A. Moubayed, A. B. Nassif and A. Shami, "Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1803-1816, June 2021, doi: 10.1109/TNSM.2020.3014929. https://doi.org/10.1109/TNSM.2020.3014929

[14] Yan, Hao & Sergin, Dorukhan & Brenneman, William & Lange, Stephen & Ba, Shan. (2021). Deep Multistage Multi-Task Learning for Quality Prediction of Multistage Manufacturing Systems. 10.48550/arXiv.2105.08180. https://doi.org/10.48550/arXiv.2105.08180

[15] Vu-Viet, Thang & Pashchenko, Fedor. (2019). Multistage System-Based Machine Learning Techniques for Intrusion Detection in WiFi Network. Journal of Computer Networks and Communications. 2019. 1-13. 10.1155/2019/4708201. https://doi.org/10.1155/2019/4708201