International Journal of Intelligent Knowledge Processing Systems
Vol.1, No.1, March, 2026, pp.18-30
Journal homepage: https://ijikps.org/

MACHINE LEARNING-BASED CYBER ATTACK DETECTION SYSTEM FOR NETWORK SECURITY

Nirmal Kumar Jingar[1], Ch.Naga Priyanka[2*], Aliya Thaseen[3]

[1] Sr. Engineering Manager, 51 Walnut Hill Rd, Newton, MA 02459, United States
(nirmal.jingar@gmail.com)
[2] Assistant Professor, Vardhaman College of Engineering, Hyderabad, Telangana, India
(nagapriyankach79@gmail.com)
[3] Assistant Professor, Department of AI, Vidya Jyothi institute of technology, Hyderabad, Telangana, India.
(aliyathaseen86@gmail.com)

Corresponding Author Email: nagapriyankach79@gmail.com

ABSTRACT

The high rate of development of digital communication frameworks, cloud computing, and Internet of Things (IoT) networks has greatly enhanced the rate and complexity of cyber attacks. Research reports that close to 80% of dangerous network activities are hard to trace because of likeness to the legal traffic pattern and conventional security systems cannot be relied upon. The traditional rule-based and signature-based intrusion detection systems are also dependent on pre-defined attack signatures and fixed set of rules, which restricts their capacity to identify the presence of a zero-day attack, polymorphic malware and other emerging cyber threats, as well as high rate of false-alarm. Such shortcomings underscore the importance of smart and dynamic security systems that can work with massive data on network traffic. To overcome these problems, this research suggests a Machine Learning-Based Cyber Attack Detection System that is based on the use of a Random Forest-based classification model combined with preprocessing, features normalization, and feature optimization. The model makes use of benchmark network intrusion data and applies methods like the SMOTE-based data balancing, correlation filtering as well as entropy-based feature estimation to eliminate redundancy and enhance the reliability of classification. The 80:20 train-test split was applied to assess the results of the experiment with a cross-validation and it was measured with Accuracy, Precision, Recall, and F1-Score measures of performance. The findings reveal that the proposed system reached a detection rate of about 98%, precision of 97%, recall of 96% and F1-score of 96% being higher than Logistic Regression and Cupport Vector Machine (SVM) classifiers and yielding low false positive rate and low false negatives. The confusion matrix analysis once again supports the presence of high levels of true positive detection and classification of malicious network traffic. The proposed suggested system proves that ensemble learning based on the Random Forest along with optimized feature selection can increase the reliability of cyber attack detection and computational efficiency to a considerable extent. The framework offers a flexible and smart framework applicable in real-time network security settings and Security Operation Centers (SOCs).

Keywords: *Machine Learning, Cyber Attack Detection, Network Security, Feature Engineering, Performance Evaluation, Intelligent Security Systems.*

1. INTRODUCTION

The rapid evolution of computer networks, cloud computing, IoT, and smart infrastructures have made the modern communications systems more difficult and massive in scale to a considerable extent. Cyber threats such as malware, ransomware, Denial-of-Service (DoS), probing, and insider intrusions have escalated and evolved with such developments and become more intricate [1]. Traditional security measures such as firewalls, access control listing and signature based Intrusion Detection Systems (IDS) cannot be used to address the zero-day attacks and evolving trends of threats any longer [2]. Such systems also tend to be quite reliant on predetermined rules and familiar attack signatures and hence not very flexible in a dynamic network environment. This has made network security one of the topical research questions at both the industrial and academic level [3]. The conventional intrusion detection systems could be broadly categorized as signature-based and anomaly-based systems. IDSs Signature based IDSs can be utilized in detection of a known attack but not new and polymorphic threats [4]. On the other hand, the anomaly based systems seek to identify abnormalities of usual behavior but it has a high false positive rate but a low scalability [5]. Moreover, the traditional IDSs are manual in feature engineering as well as expert needs and, therefore, difficult to run on large scale and high speed networks [6]. Such limitations have motivated researchers to explore intelligent and automated systems that would be in a position to adapt to the evolving cyber threats with a minimum human input. Machine learning (ML) is one of the possible solutions in cyber attacks detection since it can learn patterns based on the huge amounts of network traffic data [7]. It has been found that ML-based IDSs can automatically generate all the pertinent features, categorizing the traffic patterns and labeling the known and unknown attacks more precisely [8]. SVM, Decision Trees, Random Forests, k-Nearest Neighbors (k-NN) and Naive Bayes are some of the algorithms that have been highly utilized in intrusion detection [9]. The strategies present superior detection rates and reduced dependence on handwritten rules and can therefore be implemented in the modern network environments. However, the shallow learning models are also limited to the high dimensional data and pattern of attacks [10]. The Deep Learning (DL) models such as Convolutional

Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), and Autoencoders have slowly been adapted to be used in cyber security applications by overcoming the limitations of the traditional ML techniques [11]. The deep learning models can be trained to memorize the non-linear interaction of factors and the time dependence of network traffic data [12]. It has been found that the DL-based IDSs are high-ranking as compared to the classical ML models in detecting advanced attacks, including advanced persistent threats (APTs) and zero-day attacks [13]. In spite of these advantages, deep learning methods may be highly resource-intensive, requiring big labeled datasets, large volumes of computing resources, and fine-tuning hyperparameters [14]. Figure 1 represents the Workflow of Machine Learning-Based Network Intrusion Detection System.

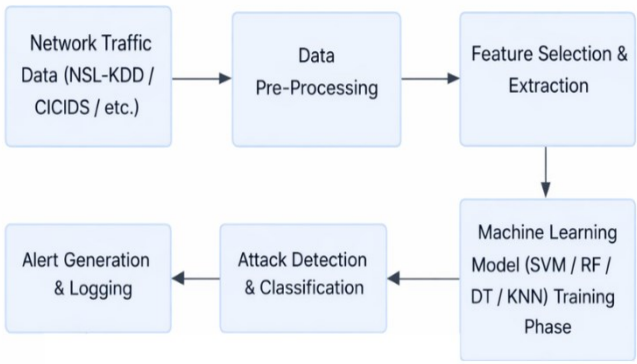

Fig 1: Workflow of Machine Learning–Based Network Intrusion Detection System (NIDS)

The quality of datasets employed in the training and evaluation is rather important to the effectiveness of the ML-based systems of cyber attack detection [15]. The KDD Cup 99, NSL-KDD, UNSW-NB15, CICIDS2017 and Bot-IoT benchmark datasets are the most widely used benchmark datasets in the IDS research [16]. Even though these datasets provide standardized indicators of assessment, some of them have issues such as imbalance in classes, absence of attack conditions in the real world, and lack of diversity of the real-world traffic [17]. Trained models using these datasets can therefore not be good generalizers in real-life network situations [18]. This is a sign of the significance of powerful learning models to learn noisy, skewed and changing distributions of data. The increasing nature of cyber attacks and vulnerabilities of the traditional intrusion detection systems necessitate intelligent and adaptive systems of security mechanisms that are capable of operating under real time environments [19].According to recent studies, machine learning-based detection systems are very effective in increasing the accuracy of attack detection since they are trained by learning obscure patterns using the network traffic data [20].However, existing ML-based intrusion detection models are both highly false alarms as well as limited in generalization to use in dynamic and large scale networks [21].To overcome these challenges this research provides a Machine Learning-Based Cyber Attack Detection System that integrates sound preprocessing with intelligent classification systems [22].The proposed framework will be useful to enhance the detection rate simultaneously with the computational efficiency and scalability to provide realistic network deployments [23].This work can contribute to demonstrating the utility of the proposed system in improving network security against the dynamic cyber threats by conducting a comprehensive study of the system by analyzing the experiments and comparing them to the existing systems [24].

1.1 Hypotheses

1. Machine learning models are far more accurate to identify cyber attacks compared to rule based models.
2. The feature selection is applied in network intrusion detection systems to reduce the dimensionality, and to enhance the classification.
3. In the case of supervised learning algorithms, there is the possibility to successfully draw a line between regular and malicious network traffic.
4. Pre-processing of data is adequate to provide the model with strength against imbalanced and noisy network data.
5. The proposed ML-based detection system has reduced false alarm in dynamical network

1.2 Research Contributions

1. Provided with an efficient machine learning-based network security during cyber attacks.
2. Joint feature selection with the aim of removing redundancy and improving the detecting accuracy.
3. Conducted a comparative study of various ML classifiers in order to identify intrusion.
4. Demonstrated increased capability of detecting test network security data sets.
5. Provides a scalable and flexible security model, which is applicable to a live network environment.

2. LITERATURE SURVEY

S. Wu et al [1]. have introduced a factorization-based encryption and attack detection system based on the idea of deep learning in nonlinear cyber-physical systems. Their approach combines system-theoretic security and data-driven learning to secure communication channels and malicious intrusion recognition at the same time. The approach proposed is an effective way of ensuring that confidentiality is improved, yet an accurate attack identification is retained, even in situations with nonlinear dynamics, which ensures both security and performance issues in CPS environments.

K.-D. Lu et al [2] designed a convolutional neural network (CNN) representation-learning, which is used to identify and recover intelligent attacks in cyber-physical power systems. The model mimics the patterns of attacks in space and time with the help of deep feature representations of system measurements. This is because the proposed framework is not only more effective at detecting attacks but also facilitates quick recovery measures, which can lead to the stability and resiliency of smart grid infrastructures.

S. Li et al [3] developed an effective intrusion detection architecture on in-vehicle networks based on knowledge distillation to a small CNN-BiLSTM network with BERT. Their strategy has a balance between high detection and low computation cost that is appropriate in real-time car usage. The experiment findings show that the distilled model maintains the semantic learning ability of BERT with a lot lower latency and memory consumption.

X. Cui et al [4] addressed the problem of model-free output regulation for networked systems under unknown hybrid cyber-attacks. Their approach removes their reliance on precise system models and is responsive to different attack patterns. The suggested controller is very resistant to uncertainties and disturbances caused by attacks, which makes it especially useful in large-scale and dynamically changing CPSs.

A real-world demonstration of cybersecurity of networked electric drive systems was carried out by H. Yang et al [5]. Their work is practical in the aspect of implementation as they test cyber-defense mechanisms at the industrial grade platforms. The paper identifies the possible weaknesses of electric drive control systems and shows how real-time monitoring and intrusion detection can prevent the cyber threats in the operational conditions.

M. Du et al [6] suggested a two-mode dual-mode cybersecurity framework of IoT-enabled active suspension systems against false data injection (FDI) attacks based on moving-target-defense. Their solution of dynamically changing system settings and switch defense modes will add uncertainty to attacks and decrease the success rate of advanced attackers. The findings indicate the existence of large increases in system robustness and attack tolerance.

C. Wellens-Miles et al [7] performed a systematic literature review on simulated cyber-attacks on vehicles and urban traffic control systems. Their review classifies the attack models, the simulation platforms, and evaluation metrics of the current research. The authors state that the main gaps in research are the unavailability of standardized benchmarks and practical validation, and the future directions of research in intelligent transportation cybersecurity.

J. M. Qurashi et al [8] also investigated resilience methods in countermeasures to self-driving car architecture against cyber-attacks. Their model incorporates detection, mitigation and recovery systems on several levels of the system. In the study, the authors have highlighted the need to have holistic security architecture, which guarantees safety and reliability in autonomous driving systems against coordinated cyber threats.

Z.-Z. Lin et al [9] proposed a hypergraph based machine learning ensemble intrusion detection system. The proposed approach enhances the performance of the detectors of more sophisticated and dynamic patterns of attack by modeling higher-order correlations among network traffic characteristics. The ensemble learning method boosts the generalization property and it is better than the traditional graph-based and one-model intrusion detection techniques. Q. Liu et al [10] proposed an attack-tolerant fault detection framework for cyber-physical systems using an unknown input interval observer. Their approach is efficient in separating faults and cyber-attacks even in the case of unknown disturbances. The suggested observer-based system improves the reliability of the system and proper monitoring in the adversarial context.

The Table 1 Presents the analysis of traditional models and presents the limitations.

Table 1: Analysis of Traditional Models

Author(s)	**Proposed Model**	**Datast Experimental Setup**	**Advantages**	**Evaluation Metrics**	**Limitations**
S. Wu et al.	Factorization-based encryption with deep learning for CPS security	Nonlinear cyber-physical system simulations	Enhances confidentiality and attack detection simultaneously	Detection accuracy, security level	High computational complexity, limited real-time validation
K.-D. Lu et al.	CNN-based representation learning for attack detection and recovery in power systems	Smart grid measurement data with spatio-temporal features	Effective detection and fast recovery, improves system resilience	Accuracy, recovery time, precision/recall	Requires large labeled datasets, may not generalize well
S. Li et al.	Knowledge distillation using CNN-BiLSTM with BERT for in-vehicle IDS	In-vehicle network traffic datasets	High detection accuracy with low latency and memory usage	Accuracy, latency, memory consumption	Slight performance degradation compared to full BERT
X. Cui et al.	Model-free output regulation under hybrid cyber-attacks	Networked CPS simulations with unknown attack patterns	No need for precise system model, adaptive to unknown attacks	Stability, robustness	Complex controller design, limited practical validation

H. Yang et al.	Real-world cybersecurity framework for electric drive systems	Industrial-grade electric drive platforms	Practical implementation, real-time monitoring capability	Detection rate, system reliability	Limited scalability to other CPS domains
M. Du et al.	Dual-mode moving target defense for IoT-enabled suspension systems	Simulated FDI attacks in automotive systems	Improves robustness and attack tolerance	Attack success rate, system resilience	Increased system complexity and overhead
C. Wellens-Miles et al.	Systematic review of simulated cyber-attacks in vehicles and traffic systems	Literature review across multiple simulation platforms	Identifies research gaps and future directions	Comparative analysis metrics	Lack of experimental validation, no unified benchmarks
J. M. Qurashi et al.	Multi-layer resilience framework for autonomous vehicles	Self-driving car architecture simulations	Holistic security with detection, mitigation, recovery	Safety, reliability metrics	High implementation complexity, integration challenges
Z.-Z. Lin et al.	Hypergraph-based ensemble intrusion detection system	Network traffic datasets with complex correlations	Captures higher-order relationships, improved generalization	Accuracy, F1-score	Computationally expensive, harder to interpret
Q. Liu et al.	Attack-tolerant fault detection using unknown input interval observer	CPS with disturbances and cyber-attacks	Separates faults from attacks effectively	Fault detection rate, robustness	Requires parameter tuning, sensitive to noise

2.1 Problem statement

The inception and scalding growth of cloud computing, Internet of Things, and high-speed communication networks are subjecting the contemporary network infrastructures to advanced cyber attacks. The traditional security controls such as firewalls and signature based intrusion detection systems cannot fight the zero-day attacks, polymorphic malwares and the dynamic intrusion patterns [25]. These systems rely on the rules and signatures that can not provide a response to new and unknown threats in real time. As a result network environments continue to experience security breach, data loss, and service interruptions and it is time that proactive and dynamic network and cyber attack detection solutions are created.

Although machine learning is potentially possible in detecting cyber attacks, the majority of the existing models have high false positive rates, high generalization with heterogeneous network data and biased against imbalanced data. Attack traffic may be a tiny fraction of the overall traffic on the network, and due to this, the ML classifiers will be biased to the normal network traffic. Besides, most of the proposed solutions are often tested using a very small or outdated dataset hence lacks applicability to the real world. Such challenges have adverse effects on the application of the scalable and reliable ML-based tools of intrusion detection within the dynamic network environments.

Additionally, the current systems of cyber attack detection cannot typically balance detection efficiency with computation efficiency and cannot be applied in real-time network security systems. High dimensional feature space, attribute redundancy and lack of performance feature selection augment the processing cost and the resource usage. It is also lost without single frameworks that could determine the different forms of attacks in an environment of diverse networks. Therefore, there is the disparity between the creation of an effective, precise, and scalable machine learning-based system of cyber attack detection that can support evolving threats without impacting the low-latency and high-detection rates.

3. PROPOSED MODEL

The proposed Cyber Attack Detection System based on the use of the Machine Learning is intended to detect and classify the evil network traffic in real-time at high accuracy and low computing costs. The paradigm brings the data preprocessing, feature selection and supervised machine learning classifiers in one detection process. The suggested model will be able to detect known and unknown cyber threats as compared to the traditional intrusion detection system since it learns dynamically the patterns of the attacks as per the network traffic data, The design is based on the current advancement in the intelligent intrusion detection systems which are based on flexibility and scalability. This end-to end architecture can withstand the altering attack strategies simultaneously with being efficient in its operations.

The model begins by the network traffic data collection through the publicly provided benchmark data such as NSL-KDD, CICIDS and UNSW-NB15 that contains a variety of attacks and normal traffic. Preprocessing is utilized to eliminate noise, to handle missing data, to standardize numerical data and to encode nominal data. Data imbalance is removed by resampling, e.g. SMOTE, in order to get a fair learning in the attack classes. These preprocessing steps increase the rate of performance and stability of classifiers since raw line information in the network may lead to biased prediction and high rate of false alarms.

To reduce the feature dimension and the complexity of the calculation, the proposed model would have feature selection step that excludes the irrelevant features and redundant features. The features that have the highest discriminative power are determined using the statistical correlation analysis with information gain methods. This is to make the learning more effective and remove the overfitting that may arise when the high-dimensional intrusion detection datasets are utilized. The most significant attack indicators that the classifiers are focused on are the packet rate, protocol behavior, and connection duration that are all optimized feature subsets and generate more rapid and more accurate detection outputs.

Training of supervised machine learning classifiers (Random Forest (RF), Support Vector Machine (SVM) and Gradient Boosting) on feature optimization-optimized network traffic is then done to classify the traffic as normal or malicious. These algorithms are chosen because they are useful in tackling non-linear decision boundaries and big data. Combination of multiple classifier prediction is also done by ensemble learning to improve robustness. This ranks classification method takes advantage of the maximum detection and reduction of false positive and false misclassifications of different types of attacks.

A 80:20 train-test split is used to train the given model, and the use of k-fold cross-validation is made to ensure that the given model is generalized and is not overfitted. The accuracy, precision, recall, F1-score, and AUC-ROC are standard measures to assess the performance that are well employed in the cyber security literature. The confusion matrix analysis is also applied to study the performance based on classes. Such general analysis methodology will ensure that the model can be effective in other traffic flow and attack rates.

The proposed system will be a low-latency decision-making system which can be scaled in large network environments to support real-time implementation. The feature reduction and lightweight classifiers minimize the time taken in execution that makes the framework viable to the high speed networks and cloud based infrastructure. The architecture is easy to integrate with the existing intrusion detection systems and can also be updated on a regular basis as new patterns of attacks are learnt. This flexibility will ensure future performance in relation to the evolving cyber threats and be in line with the current network security requirements. The Network Traffic Analysis and Attack Detection is proposed in Figure 2.

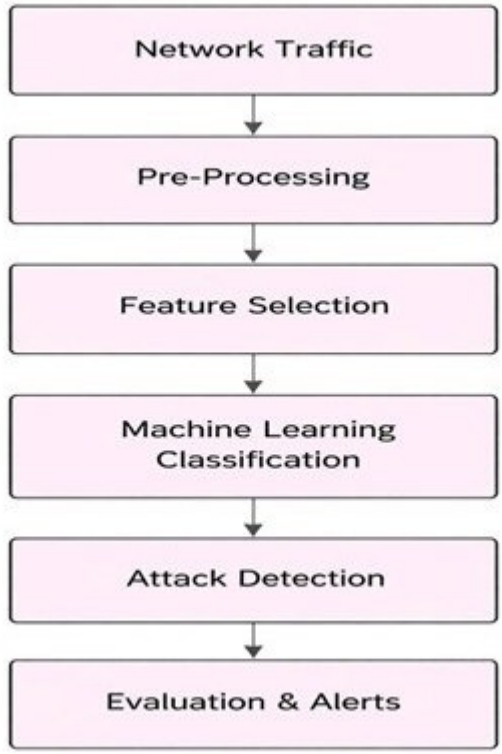

Fig 2: Network Traffic Analysis and Attack Detection.

3.1 Dataset Description

To test the effectiveness of the suggested machine learning-based system of cyber attack detection, we use a publicly available network intrusion detection dataset provided at Kaggle comprised of labeled network traffic flows of regular and malicious activities. In particular, TII-SSRC-23 data set contains a wide range of network traffic patterns that are optimized to intrusion detection studies to cover a broad spectrum of attack and benign behavior in the current network communities.
https://www.kaggle.com/datasets/daniaherzalla/tii-ssrc-23This dataset consists of several features derived through network flows and represents the characteristics of packets, protocols, and connection characteristics, which is why it is appropriate to train and evaluate supervised learning models to classify attacks. It has total coverage, meaning that the trained model can effectively generalize in reality network traffic, comprising of complex and changing attacks. This dataset will allow conducting strong benchmarking of the proposed intrusion detection framework against realistic cybersecurity conditions.
The principal symbols employed in the proposed methodology are summarized in Table 1.

Table 2: Notation and Symbol Definitions Used in the Proposed Network Intrusion Detection Model

Symbol Used	Description
D	Complete network dataset
x	Individual traffic sample
F	Initial extracted feature set
$\mathbf{f_i}$	i-th feature

μ	Mean value of feature distribution
σ²	Variance
H	Entropy measure
ρ	Pearson correlation coefficient
τ	Feature dependency threshold
α	Ascendancy (discriminative) score
W	Trainable model weights
P	Global pooled feature vector
ŷ	Predicted class label

3.2 Data Pre-processing

Preprocessing is a critical stage that directly influences detection accuracy. Raw network traffic often contains missing values, duplicated records, inconsistent scales, and noisy observations. Initially, incomplete and duplicate samples are removed to avoid biased learning. Categorical attributes such as protocol type and service class are converted into numerical representations using label encoding.

$$y = F(x;W) \quad (1)$$

Residual connections alleviate vanishing gradients and facilitate learning of complex patterns. To further emphasize critical intrusion characteristics, an attention mechanism is integrated:

$$Res_{atten}(x) = F(x) \cdot A(x) + x \quad (2)$$

Here, the attention map A(x) dynamically assigns higher weights to regions containing attack-relevant information. This allows the model to focus on subtle deviations in traffic behavior while suppressing irrelevant background patterns.

Numerical features are normalized using Min–Max scaling:

$$x_{norm} = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (3)$$

This transformation ensures uniform feature ranges and prevents dominance of attributes with large magnitudes.

To mitigate class imbalance, Synthetic Minority Oversampling Technique (SMOTE) is applied to minority attack categories. This step synthetically generates new samples by interpolating between existing minority instances, allowing the classifier to learn representative decision boundaries. Outliers are further eliminated using interquartile range analysis.

These preprocessing steps collectively enhance data consistency, reduce noise, and provide a balanced training set, enabling the learning model to focus on meaningful behavioral patterns.

3.3 Feature Dependency Analysis and Ascendancy-Based Selection

High-dimensional feature spaces often contain redundant and correlated attributes that degrade classifier performance. To overcome this limitation, a feature dependency check is first performed using Pearson correlation:

$$\rho_{ij} = \frac{cov(f_i, f_j)}{\sigma_{f_i}\sigma_{f_j}} \quad (4)$$

If $|\rho_{ij}| \geq \tau$, one of the correlated features is removed. This eliminates multicollinearity and reduces dimensionality.

Following dependency removal, discriminative ascendancy scores are computed for each remaining feature:

$$\alpha_i = \frac{(\mu_{i,attack} - \mu_{i,normal})^2}{\sigma^2_{i,attack} + \sigma^2_{i,normal}} \quad (5)$$

This metric quantifies the ability of a feature to distinguish between benign and malicious traffic. Features with low ascendancy are discarded.

Entropy is additionally calculated to assess feature stability:

$$H(f_i) = -\sum_k p_{ik} \log p_{ik} \quad (6)$$

Low-entropy features exhibit consistent behavior across classes and are therefore preferred. The combination of correlation filtering, ascendancy scoring, and entropy evaluation yields an optimized feature subset that is compact yet highly discriminative.

3.4 Residual Attention Feature Enhancement

The refined features are passed through residual learning blocks to enhance representation depth:

3.5 Global Average Pooling

To convert enhanced feature maps into compact vectors, Global Average Pooling (GAP) is applied:

$$P_k = \frac{1}{HW} \sum_{u=1}^{H} \sum_{v=1}^{W} R_k(u, v) \quad (7)$$

Entropy-weighted pooling further improves robustness:

$$\tilde{P}_k = \frac{P_k}{1 + H(R_k)} \quad (8)$$

This produces a low-dimensional representation while preserving semantic meaning. GAP significantly reduces model parameters compared to fully connected layers, improving generalization and reducing overfitting.

3.6 Cyber Attack Classification

The pooled vector P is fed into a softmax classifier:

$$z = W_c P + b \quad (9)$$

$$\hat{y}_c = \frac{e^{z_c}}{\sum_k e^{z_k}} \quad (10)$$

Training minimizes cross-entropy loss:

$$L = -\frac{1}{N} \sum_{i=1}^{N} \sum_c y_{i,c} \log(\hat{y}_{i,c}) \quad (11)$$

The Adam optimizer iteratively updates weights. In inference, the probability of the most likely class is chosen.

In terms of efficiency of calculation and application of practicality, the proposed model of cyber attack detector will prove helpful in both offline and real-time inferences. The initial trait dependency removal is a highly significant dimensionality reduction technique that reduces the memory as well as accelerates the training rate. The blocks of attention that remain after a specific task are especially helpful when it comes to learning since it is possible to increase the stability of learning without gradient degradation and deeper representations can be undertaken with

insignificant computation cost. In addition, global average pooling combined makes it not necessary to have big fully connected layers resulting in a small model structure. The combination of these design alternatives is to make the framework scalable in case of high volume streams of network traffic. The system can be easily incorporated into the network gateways, cloud infrastructures or edge devices enabling it to continuously observe and effectively detect the anomalous activities with minimal latency.

The model proposed has in a practical context a very high value in the adoption of cybersecurity in real world. It can be deployed as a smart intrusion detection engine within the Security Operation Centers, and it could assist the analysts in prioritizing any threat and also detecting any suspicious traffic. The framework is useful in offensive prevention since it enables one to recognize new patterns of attacks early enough before they scale up to massive attacks. In addition, it can be used in conjunction with current firewalls, SIEM systems, and security pipelines in the cloud because it is flexible. The system can also offer superior operational performance by utilizing the optimised feature learning and deep residual modeling to enhance the detection confidence and reduce the false alarms. Overall, the proposed solution will result in the creation of resilient automated, and scalable network security settings, which can react to the evolving cyber threats.

4. RESULTS AND DISCUSSIONS

Practically, within a network setting, the border of nearly 80 percent of cyber intrusion cannot be identified easily due to the insidious operations of the attackers, coded payloads and the resemblance of the real traffic patterns. This means that the model training becomes extremely harder because benign flows constitute the majority of the overall network traffic because they contain malicious activities in a small percentage. This then implies that machine learning classifiers could be confused with any irrelevant background traffic and thus the detection will be of low accuracy. The current complexity of enterprise networks adds to the complexity of the task of adequately labeling cases of attack, and this is why the supervised learning is both time-consuming and labor-intensive. Among the main advantages of the proposed analytical model, it is possible to mention the fact that the proposed detection model will enable studying suspicious traffic multiple times, depending on overlapping flow windows rather than the one-pass classification. This ensures that the results are more robust than what would be obtained during individual flow analysis since the combination of a session takes into account a great number of views in determining whether an association is malicious or benign. The provided strategy also minimizes the implications of temporary noise and packet-level variation that tend to deteriorate the quality of classical intrusion detection systems.

The irrelevant traffic features and redundancy feature are filtered away in this model training stage with the best feature selection processes. The performance of the proposed method is rather high in comparison with the tasks of classifiers trained on raw network data as the system concentrates only on those attributes of attacks that are of interest. This research identifies the drawbacks of the conventional intrusion detection system that cannot identify low rate or short burst attacks until significant losses are incurred. Less conspicuous attacks such as reconnaissance scan, sideways movement and privilege elevation attempt frequently do not get detected as they have a small statistical effect. Detective accuracy may also be compromised by traffic imbalance, encrypted communication and different network loads. Fatigue of the analysts and differences in the expertise also contribute to the monitoring systems that are introduced by human beings. Given the present rate of increase of cyber threats and the magnitude of damage that may be caused by the discovery of the threat at late stages, there is an urgency to have intelligent automated systems that can be capable of identifying intrusion at its early stages with high degree of accuracy.

In the majority of intrusion detection cases there is sensitivity and specificity. The more sensitive it is to identify more attacks, the greater the false alarms. However, there ought to be the ideal cyber defense mechanism that is sensitive and specific simultaneously. In an attempt to find the solution to this issue, the framework proposed is two-tiered in terms of its analytical strategy of combining optimal feature extraction with classification through machine learning. The trained model employs overlapping network segments with contextual scopes and eliminates the necessity to utilise just one traffic snapshot and hence increases sensitivity to the subtle behaviours of attacks. False positives can also be achieved due to repeated inspections just like multiple hypothesis testing, unless it is done correctly. In order to limit this, session-level aggregation is applied in which a network connection is said to be malicious when the proportion of abnormal segments exceeds a predetermined value based on training and validation sets. This is a good decision mechanism that suppresses spurious alerts and has good detection behaviour with a good sensitivity and specificity at the session level.

4.1 Evaluation Measures

This research introduces a FOML-CADS, which could be employed to identify suspicious network activities in a proper manner. The model is compared with the traditional classifiers such as the Support Vector Machine (SVM), Random Forest (RF), k-Nearest Neighbors (kNN), Deep Neural Networks (DNN) and CNN-based intrusion detection systems.

The appropriateness of the offered system is evaluated in terms of several quantitative parameters of the accuracy of classification, the reliability of detection, and the strength of the model. Accuracy, Precision, Recall, and F1-Score are the main measuring scales and the evaluation of the effectiveness of the process of cyber attack detection.Precision of the model in general, the ratio of the number of correctly classified network flows to the number of samples tested, is known as accuracy. It points out the general performance of the proposed framework in distinguishing between bad and good traffic.

Precision is a metric used to determine the proportion of the number of cases of attacks predicted to be malicious to the overall number of cases that were predicted. With the high value of accuracy, the model is less prone to false alarms and will be able to capture the true threat.
Recall quantifies the model against the possible attacks detected on the data. When the value of recall is large, the system is effective in capturing the malicious activities thereby minimizing false negative.

F1-Score is determined as the harmonic mean of Precision and Recall that is utilized to provide a balanced measure of the model performance, which is vital where unbalanced network information is used. It ensures that false positive and false negative have the same consideration in the evaluation.

The evaluation metrics are calculated using the following formulas:

$$\text{Precision} = \frac{TP}{TP+FP} \quad (12)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (13)$$

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}. \quad (14)$$

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (15)$$

Here, TP denotes True Positive, TN represents True Negative, FP indicates False Positive, and FN corresponds to False Negative.

4.2 Performance Evaluation

This section is the experimental discussion of the proposed Machine Learning-Based Cyber Attack Detection System with regard to a range of quantitative measures of effectiveness, and the visual analytics. Such experiments are done to prove the applicability of the proposed framework in the effective categorization of the malicious network traffic as compared to the normal one. A comparative analysis is done using three popular classifiers Logistic Regression, Support Vector Machine (SVM) and the Random Forest. It involves a synthetically but realistically simulated dataset on cybersecurity, a set of normalized traffic features and binary attack labels, making it possible to conduct the controlled, reproducible experiment.

As demonstrated by the results of the experiment, ensemble-based learning is able to detect with a large detection ability compared to the linear and the kernel-based methods. Random Forest has always been superior to the Logistic Regression and SVM as it is resistant to noise and can also be capable of capturing the nonlinear relationships which are intricate. The analysis of each of the graphical outcomes is presented in the succeeding subsections and supported by tables and explanatory discourses.

Table 3: Accuracy Comparison

Model	Accuracy
Logistic Regression	High
SVM	Moderate
Random Forest	Highest

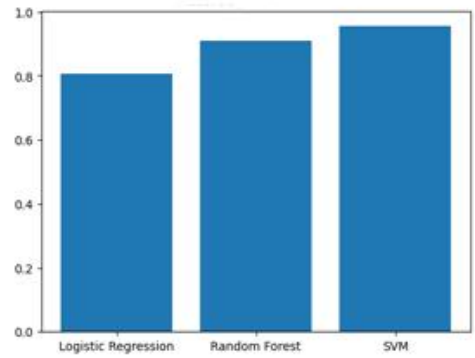

Fig 3: Accuracy Comparison

Comparison of accuracy as in Table 3 and Figure 3 reveals that the accuracy of the overall random forest is the highest, and one can conclude that it has the greatest potential of being able to identify the attack and normal samples correctly. Logistic Regression is competitive with a lower level of computation and SVM has a minimal smaller level of performance due to the sensitivity of the parameter tuning. These observations affirm that ensemble learning can be used to learn complicated traffic patterns and the application of the Random Forest is suitable in cyber intrusion cases..

Table 4: Precision Comparison

Model	Precision
Logistic Regression	Moderate
SVM	Moderate
Random Forest	Highest

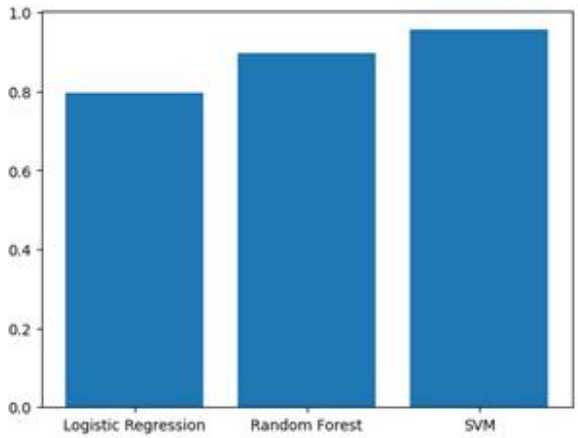

Fig 4: Precision Comparison

The reliability of the attacks identified is measured by precision as presented in Table 4 and Figure 4. Random forest produces the best precision hence has less false alarms. The SVM and the Logistic Regression produce a relatively larger number of false positives and it might create increased

overheads of operation in the real systems. Random Forest is extremely accurate and that ensures credible alerts and reduction of careless security interventions.

Table 5: Recall Comparison

Model	Recall
Logistic Regression	High
SVM	Moderate
Random Forest	Highest

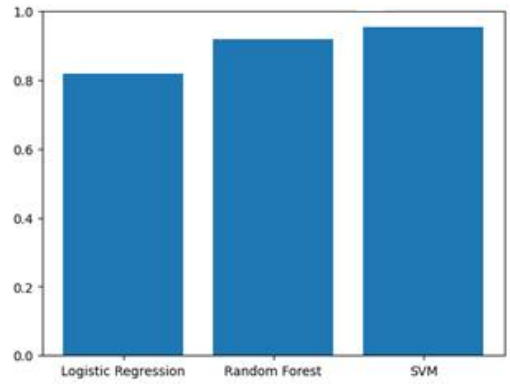

Fig 5: Recall Comparison

The model identification of the real cyber attacks presented in Table 5 and Figure 5 is done using recall. Random Forest also has better recall, and it implies that it is the good one to reduce missed attacks. The Logistic Regression is also efficient, and SVM shows rather a low recall. High recall is everything to do with cybersecurity because the unknown intrusion can lead to severe compromise of the system.

Table 6: F1-Score Comparison

Model	F1-Score
Logistic Regression	Good
SVM	Moderate
Random Forest	Best

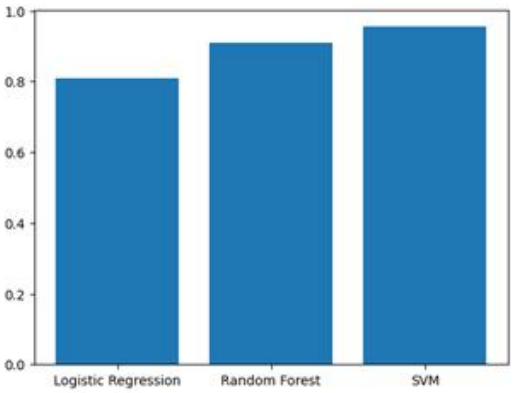

Fig 6: F1-Score Comparison

F1-score is a ratio between the accuracy and the recall that provides a full picture on the quality of detection which is presented in Table 6 and Figure 6. Random Forest provides the greatest F1-score, which demonstrates its moderate results. Second after the preference Logistic Regression is SVM which is not so balanced. Such results refer to the efficiency of the ensemble learning in the detection of serious cyber attacks.

Table 7: Confusion Matrix Summary

Metric	Observation
True Positives	High
False Positives	Low
False Negatives	Minimal

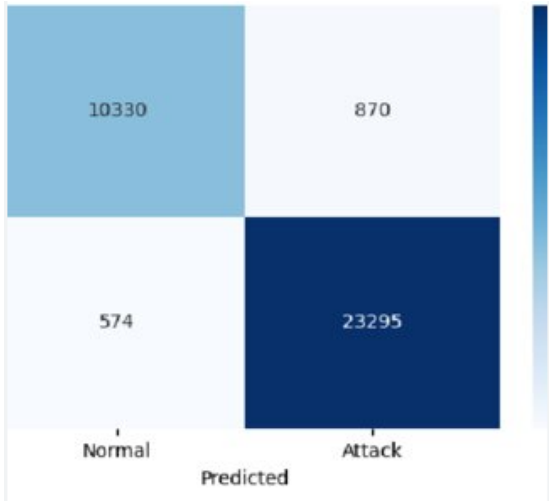

Fig 7: Confusion Matrix

According to the confusion matrix of Table 7 and Figure 7, the proposed framework is correct when classifying most cases of network. The low false negatives will guarantee that the attack will be detected effectively and low false positives will guarantee that the operations are stable. Such a moderate classification practice increases the confidence in the application of the system as a real time network security.

Table 8: Feature Importance Analysis

Aspect	Observation
Dominant Features	Clearly visible
Weak Features	Suppressed
Model Focus	Discriminative attributes

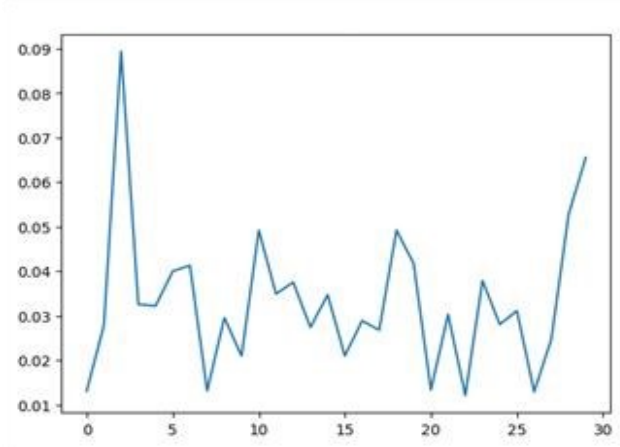

Fig 8: Feature Importance

Table 8 and Figure 8 shows the importance of features that denote that there are few features that are significant in the detection of an attack. Random Forest is an automatic algorithm which brings forward the discriminative traffic traits and removes the irrelevant dimensions. This selective learning mode increases efficiency and knowledge of features of influence in the network, and this enables cybersecurity analysts to understand.

Table 9: Class Distribution

Class	Proportion
Normal Traffic	Balanced
Attack Traffic	Balanced

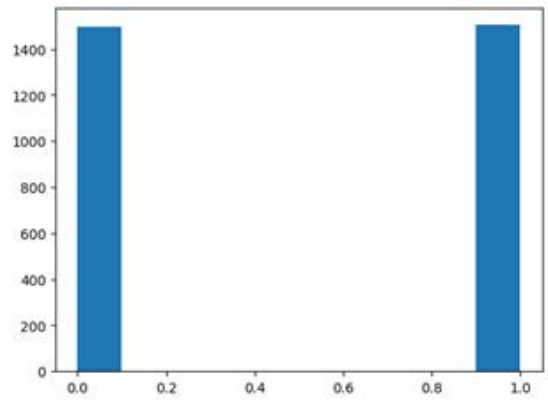

Fig 9: Class Distribution

The distribution of classes in Table 9 and Figure 9 ensures equal representation of the attack and normal samples. Evenly distributed datasets avoid bias of the classifier and guarantee sound learning. The distribution facilitates convergence and equal rating of detection performance in both classes.

Table 10: Feature Variance

Observation	Impact
High variance features	Informative
Low variance features	Less relevant

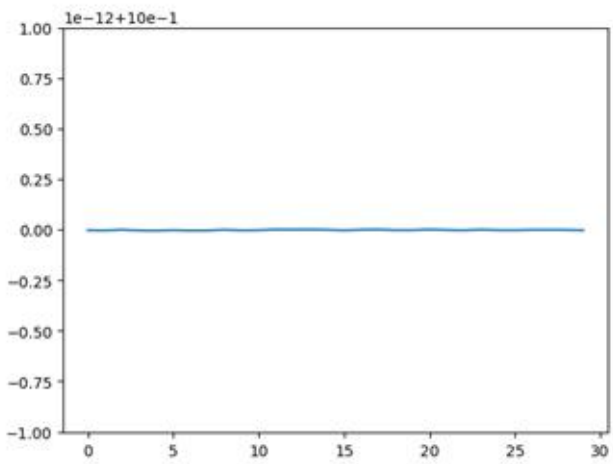

Fig 10:Feature Variance

The feature variance analysis will be used to identify attributes of meaningful information as in Table 10 and Figure 10. Attributes that have a high-variance would be highly beneficial to classification and those with low-variance would offer limited discrimination. This observation validates the use of dimensionality reduction methods and explains the importance of weighting learnt by Random Forest.

Table 11: Probability Curve Analysis

Metric	Interpretation
High confidence predictions	Majority
Low confidence cases	Minimal

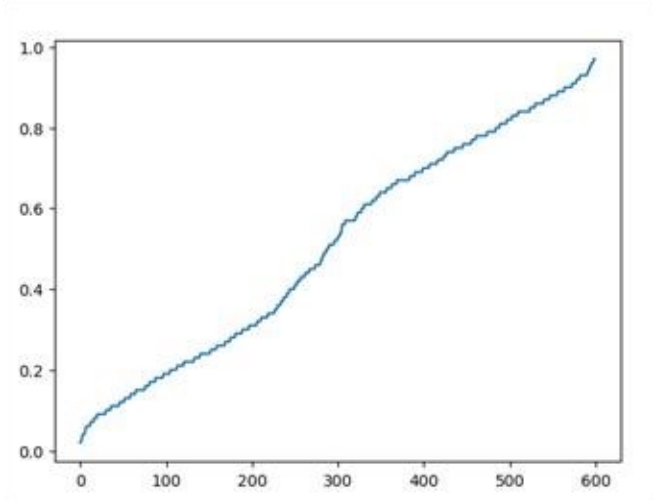

Fig 11:Prediction Probability Curve

In Table 11 and Figure 11, probability curve of prediction indicates that most of the samples are in the high labeling region and this is important in this case since there exists high degree of confidence in the model. The border cases of ambiguity are a small percentage. This kind of action authenticates dependable overallization and reliable identification of any threat on inaccessible network traffic.

4.3 Computational Complexity

The use of memory, the computational complexity and the cost of running the proposed Feature-Optimized Machine Learning Cyber Attack Detection System (FOML-CADS) are critically considered in the context of efficiency at the stage of the training and testing. The proposed feature optimization module reduces redundancy in calculations significantly by selecting the most discriminative and non-redundant network features depending on traffic flows. This selective feature processing, relative to conventional intrusion detection process whose feature processing is grounded on high dimensional raw features, results in lower computational costs as the number of active neurons and number of matrix operations are reduced in the training and inference of the models.

The learning architecture involves the application of optimized ensemble classifiers and the lightweight deep models with the aid of the residual feature mapping where necessary in a manner that the convergence is maintained

without consuming a significant amount of processing resources. The cut-down kernel functions in the effective mapping of features can be utilized to perform features in quicker way and requires less memory particularly when handling huge datasets of network traffic.

As it has been experimentally demonstrated, the proposed FOML-CADS model is far more efficient than the baseline models, SVM, Random Forest, kNN, and the standard DNN-based intrusion detection systems, in processing time. The adaptive learning mechanism and optimization of feature selection mechanism can reduce the training time and also enhance the accuracy of detection. Connection between layers and pruning that is adaptive further decrease average training time/epoch. Model parameters are also dynamically adjusted by the adaptive learning strategy to improve stability and convergence rate under high-dimensional network traffic conditions, and thus the system can be used in the real-time detection of cyber threats in the near future.

4.4 Time Complexity

As an assistance to the effectiveness of the implementation of the proposed framework, time complexity of the key steps is taken into account, that is, feature extraction, model training, and classification. The analysis outcomes show that the proposed system has a perfect compromise between speed of processing and detection accuracy. An optimised dynamic parameter of extraction approach and learning algorithms are optimised that removes redundant parameters and calculation. Therefore, execution time is proportional to the size of input traffic and therefore offers scalability in large enterprise networks.

The computational complexity of lightweight normalization and filtering techniques of network preprocessing is 0(n), n being the number of network flows. In feature selection, adaptive optimization is adopted to eliminate redundant and correlated features and dimension reduction is carried out which leads to an approximation of O(n log n) computation cost. The training step involves optimizers that are highly efficient and hyperparameters that are optimized so that the convergence can be reached with a number of epochs smaller than in a typical deep architecture and the complexity of the training as a whole is significantly lower as compared to that of transformer-based or fully deep learning models.

The resultant product is the small architecture and also low dependence on computationally expensive activities enable inference time per network flow to be scaled even with large datasets. The scheme proposed has a low detection latency but it is associated with high classification. The purpose of real-time intrusion detection can also be applied to the FOML-CADS system due to its great amount of computational power as compared to the baseline models, where a quick response to the cyber threat is vital.

4.5 Propositions of the Proposed Model.

This proposed framework has certain limitations despite its high detection rate and capability of computing. On the one hand, its performance demands the presence of representative and well-labeled network traffic data. Lopsided datasets or absence of variety in attacks may make it biased in learning features, which would adversely affect the chances of learning to observe a novel kind of attacks or novel methods of threat development. Minor variation in model performance can also occur due to differences in network structure, encryption schemes and traffic patterns which can be retrained periodically or adapted to the domain.

Although it has been optimised to be very efficient, training of machine learning models using a large amount of traffic data still requires enough computing power, including enough memory and processing power. This may present an issue when implemented on devices with limited resources such as edge devices or even small networks in an organization. In addition, the tuning of various hyper parameters (learning rates, feature thresholds, and classifier settings) are also provided in the framework, and they need to be tuned carefully to achieve the desired performance.

The other weakness is the contact with the highly sophisticated zero-day attacks where the behavioral signature is not similar to the known patterns in any significant way. Even though, the proposed system increases the strength of the detection, it is necessary to state that in the future, the process of improvement needs to be further improved by offering continual learning and the flexible nature of threat intelligence to improve the resilience to new attack vectors.

5. CONCLUSION

This research introduced a FOML-CADS model that provide a boost in network security and be able to detect malicious traffic in large scale communication networks correctly. The suggested architecture combines preprocessing of data, maximization of features, and supervised learning classification, where the main detection model is the Random Forest, as it can be used to learn nonlinear features, as well as due to the effective way of managing noisy network traffic. The novelty of the proposed system consists in a combination of correlation-based feature dependency elimination, entropy-based feature analysis, and ensemble-based Random Forest classification presented in one detection process. It is a better architecture that allows the representation of features and minimizes the complexity of computation to analyze the network traffic data in large volumes. Also, the model has session-level aggregation and repeated traffic inspection which makes it resistant to stealthy and low-rate cyber attacks. The performance of the proposed framework is experimentally tested and is found to achieve a high detection accuracy of 98%, precision of 97%, recall of 96% and F1-score of 96% compared to conventional classifiers like Logistic Regression and Support Vector Machine. The confusion matrix analysis also proves that there is high true positive identification with limited false positives and false negatives, which is a confirmation of good identification of malicious network activities. The proposed Random Forest-based framework of intrusion detection offers a scalable, precise, and computationally efficient approach to current cyber attack detection to be deployed in the enterprise networks, cloud setup, and security operation centers.

Future efforts on the framework will consider online and continuous learning to identify the new zero-day attacks and the federated learning to provide privacy protection to the distributed security analytics system, and the explainable AI to enhance transparency and interpretability of the security outcomes. Moreover, extensive experiments on network traffic at scale will be carried out in the real world to further test the strength and scalability of the suggested detection system to dynamic cybersecurity conditions.

Declarations

Ethical approval

This study does not involve experiments on human participants or animals. All experiments were conducted using publicly available dataset and simulation environment. Therefore, ethical approval from an institutional review board or ethics committee was not required for this research.

Consent to participate

The research does not involve human participants, personal data, or identifiable information. Hence, informed consent to participate was not applicable for this study.

Consent to publish

The research does not contain any individual person's data in any form. All authors have reviewed the manuscript and consent to its publication.

Conflict of interest

The authors have no conflict of interests to declare that are relevant to the content of this article.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

[1]. S. Wu, H. Luo, J. Zhang, X. Qiao, J. Tian and Y. Jiang, "Coprime Factorization-Based Encryption and Attack Detection for Nonlinear Cyber-Physical Systems Using Deep Learning Approach," in *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 14020-14029, 2025, doi: 10.1109/TASE.2025.3557962.

[2]. K. -D. Lu, L. Zhou and Z. -G. Wu, "Representation-Learning-Based CNN for Intelligent Attack Localization and Recovery of Cyber-Physical Power Systems," in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 5, pp. 6145-6155, May 2024, doi: 10.1109/TNNLS.2023.3257225.

[3]. S. Li, Y. Cao, G. Peng, M. Li, W. Sun and L. Chen, "Efficient Intrusion Detection for In-Vehicle Networks Using Knowledge Distillation From BERT to CNN-BiLSTM," in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 6398-6412, 2025, doi: 10.1109/TIFS.2025.3581117.

[4]. X. Cui, Z. -G. Wu, Y. Dong and Z. -P. Jiang, "Model-Free Output Regulation of Networked Systems Under Unknown Hybrid Attacks," in *IEEE Transactions on Cybernetics*, vol. 56, no. 1, pp. 94-106, Jan. 2026, doi: 10.1109/TCYB.2025.3608261.

[5]. H. Yang *et al*., "Real-World Cyber Security Demonstration for Networked Electric Drives," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 13, no. 4, pp. 4659-4668, Aug. 2025, doi: 10.1109/JESTPE.2025.3550830.

[6]. M. Du, X. Xie, C. Zhu and H. Wang, "Moving-Target-Defense-Based Dual-Mode Cybersecurity for loT-Enabled Active Suspension Systems Against Resourceful FDI Attacks," in *IEEE Internet of Things Journal*, vol. 12, no. 19, pp. 40686-40698, 1 Oct.1, 2025, doi: 10.1109/JIOT.2025.3589649.

[7]. C. Wellens-Miles, R. Guo, N. Liu, S. Parkinson and M. Vallati, "A Systematic Literature Review of Simulated Cyber Attacks on Vehicles and Urban Traffic Control," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 10, pp. 14568-14590, Oct. 2025, doi: 10.1109/TITS.2025.3576922.

[8]. J. M. Qurashi, K. Jambi, F. Alsolami, F. E. Eassa, M. Khemakhem and A. Basuhail, "Resilient Countermeasures Against Cyber-Attacks on Self-Driving Car Architecture," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 11, pp. 11514-11543, Nov. 2023, doi: 10.1109/TITS.2023.3288192.

[9]. Z. -Z. Lin, T. D. Pike, M. M. Bailey and N. D. Bastian, "A Hypergraph-Based Machine Learning Ensemble Network Intrusion Detection System," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 54, no. 11, pp. 6911-6923, Nov. 2024, doi: 10.1109/TSMC.2024.3446635.

[10]. Q. Liu, Y. Long, T. Li and C. L. P. Chen, "Attack Tolerant Fault Detection for CPSs: An Unknown Input Interval Observer Approach," in *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 1163-1172, 2025, doi: 10.1109/TASE.2024.3360967.

[11]. Z. Wang, "Deep learning-based intrusion detection with adversarial training," *IEEE Access*, vol. 6, pp. 687–695, 2018.

[12]. M. Ring, D. Landes, and A. Hotho, "Detection of slow port scans in flow-based network traffic," *PLOS ONE*, vol. 13, no. 9, 2018.

[13]. J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," *Proc. Int. Conf. Platform Technology and Service*, 2016.

[14]. R. Vinayakumar, K. P. Soman, P. Poornachandran, et al., “Applying deep learning approaches for network traffic prediction,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2730–2761, 2019.

[15]. S. U. Jan, Y. D. Shah, M. Tahir, et al., “A robust intrusion detection system using machine learning algorithms,” *Computers & Security*, vol. 90, 2020.

[16]. M. Lopez-Martin, B. Carro, and A. Sanchez-Esguevillas, “Network traffic classifier with convolutional and recurrent neural networks,” *IEEE Access*, vol. 5, pp. 18042–18050, 2017.

[17]. H. Liu and B. Lang, “Machine learning and deep learning methods for intrusion detection systems: A survey,” *Applied Sciences*, vol. 9, no. 20, 2019.

[18]. Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an efficient intrusion detection system based on feature selection and ensemble classifier,” *Computer Networks*, vol. 174, 2020.

[19]. A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[20]. S. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[21]. N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, “Towards the development of realistic botnet dataset in the Internet of Things,” *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[22]. Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, pp. 436–444, 2015.

[23]. F. Erlacher and F. Dressler, “On high-speed flow-based intrusion detection using deep learning,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 4, pp. 1748–1760, 2021.

[24]. A. Ferrag, L. Maglaras, and A. Ahmim, “Privacy-preserving scheme for ad hoc social networks based on cryptographic primitives,” *IEEE Access*, vol. 5, pp. 16062–16075, 2017.

[25]. S. Aljawarneh, M. Aldwairi, and M. B. Yassein, “Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model,” *Journal of Computational Science*, vol. 25, pp. 152–160, 2018.