Power System Technology
ISSN:1000-3673

Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

Enhanced Intrusion Detection System through Optimizing Neural Wavelet Transforms and Pelican Optimization Algorithm-Long Short-Term Memory Techniques

M.Ancy,
Research scholar, Department of electronics and communication engineering.
Dr.M.G.R Educational and research institute, Chennai.
Dr.M. Kumaresan,
Department of electronics and communication engineering,
Dr.M.G.R Educational and research institute, Chennai.

ABSTRACT

This research introduces an advanced intrusion detection framework employing a synergistic integration of preprocessing techniques and sophisticated machine learning models. The proposed methodology incorporates Neural Network (NN), Transverse Dyadic Wavelet Transform (TYDWT), and Fast Fourier Transform (FFT) as powerful preprocessing algorithms, refining and optimizing network datasets for subsequent analysis. Long Short-Term Memory (LSTM) networks, known for their sequence modelling capabilities, are employed for feature extraction and classification, showcasing adaptability to intricate patterns in network data. A significant contribution is proposed in the form of the Pelican Optimization Algorithm - Long Short-Term Memory (POA-LSTM), a novel algorithm designed for enhanced optimization and feature extraction. Notably, POA-LSTM demonstrates remarkable accuracy, marking a substantial advancement in intrusion detection capabilities. Additionally, the study explores the Cat Optimization Algorithm - Long Short-Term Memory (COA-LSTM), further extending the adaptability of LSTM models for intrusion detection. The holistic evaluation of the proposed framework encompasses essential metrics, including accuracy, precision, specificity and sensitivity, providing a comprehensive assessment of its performance across diverse intrusion scenarios. The results underscore the efficacy of the proposed POA-LSTM algorithm, emphasizing its capability to achieve high accuracy about 98% in intrusion detection.

Keywords: Intrusion detection; Pelican Optimization Algorithm - Long Short-Term Memory (POA-LSTM); network

1. INTRUDUCTION

An Intrusion Detection System (IDS) is a crucial component of cybersecurity that monitors network or system activities for malicious activities or policy violations. It works as a detective

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

control mechanism, providing real-time analysis of security alerts generated by applications and hardware within a network. There are two primary types of IDS such as Network-Based Intrusion Detection System (NIDS) and Host-Based Intrusion Detection System (HIDS). NIDS monitors network traffic in real-time and analyzes packets for suspicious patterns that may indicate a security breach or intrusion attempt. Placed strategically at various points within the network, such as routers or switches, NIDS examines all traffic that passes through these points. NIDS uses signature-based detection (pattern matching against known attack signatures) and anomaly-based detection (deviation from established baselines) to identify potential threats. NIDS can detect attacks and malicious activities on the network even before they reach individual hosts. HIDS resides on individual hosts or devices, monitoring system activities, files, and configurations for signs of malicious activities or policy violations. Installed on specific devices like servers, workstations, and other critical systems, HIDS focuses on the activities occurring on that particular host. HIDS employs various techniques such as log analysis, file integrity checking, registry monitoring, and kernel parameter monitoring to identify potential intrusions or unauthorized activities. HIDS can detect attacks that originate from both external sources and within the host itself.

Intrusion Detection Systems (IDS) utilize various algorithms and techniques to identify and respond to malicious activities or security incidents within a network or system. IDS compares network traffic or system behavior against predefined patterns or signatures of known attacks. Monitors active connections and compares them against a database of approved states, flagging any deviations as potential intrusions. Uses pattern-matching techniques to identify specific sequences of characters or behaviors indicative of known attacks. Establishes a baseline of normal behavior using statistical methods and flags any deviation from this baseline as an anomaly. Utilizes various machine learning techniques such as clustering, classification, or neural networks to identify patterns and anomalies in network traffic or system behavior. Profiles network traffic to establish what normal behavior looks like and identifies deviations from this profile. Focuses on user or system behavior, detecting anomalies based on deviations from established behavioral patterns. Integrates both signature-based and anomaly-based techniques to improve detection accuracy and reduce false positives. Utilizes rule-based systems and human-defined knowledge to identify patterns and anomalies, often combined with machine learning algorithms for enhanced accuracy. Utilizes rule-based or expert knowledge to detect previously unseen or zero-day attacks based on heuristic rules. Predicts potential future attacks based on current and historical data, enabling proactive measures. Analyzes flow data to identify suspicious patterns, connections, or behaviors within the network traffic. Examines network protocols for inconsistencies, unusual patterns, or non-compliance, which could indicate an intrusion attempt. Focuses on deviations from established behavioral norms without relying on predefined signatures, allowing detection of novel attacks.

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

Analyzes the content of network packets in real-time to identify malicious patterns or behavior, often used for detecting complex attacks.

While IDS algorithms are essential for identifying and responding to security threats, they do come with certain drawbacks and limitations. Signature-based IDS can only detect attacks for which signatures are predefined. New, unknown attacks (zero-day attacks) can bypass this detection method. Anomaly-based IDS may struggle to detect previously unseen threats if they do not deviate significantly from historical patterns. Depending on the heuristics used, there can be a significant number of false positives, leading to alert fatigue. Flow-based IDS focuses on network flow data and lacks the ability to inspect packet contents, missing attacks within encrypted traffic. Protocol-based IDS relies on understanding protocol specifications. Attackers can exploit protocol intricacies that are not well-known or documented. Behavioral and deep packet inspection methods often require complex algorithms and substantial computational resources, making them challenging to implement and maintain. It's important to note that while these drawbacks exist, many organizations use a combination of these IDS algorithms to create a more robust and adaptive security posture, mitigating the limitations of individual methods. Regular updates, continuous monitoring, and a comprehensive understanding of the network environment are crucial for effective IDS deployment and management.

Certainly, there are various types of cyber-attacks, each designed to exploit specific vulnerabilities or achieve particular objectives. Malicious software that attaches itself to legitimate programs and spreads when the infected program is executed. Self-replicating malware that spreads across networks without user intervention. Malware disguised as legitimate software that allows unauthorized access to the victim's system. Malware that encrypts a user's data and demands payment (ransom) to restore access. Software that secretly monitors user activity, gathering sensitive information. Phishing is fraudulent attempts to obtain sensitive information by impersonating a trustworthy entity, often via email or fake websites. Targeted phishing attacks aimed at specific individuals or organizations, often using personalized information. Phishing attacks specifically targeting high-profile individuals or executives within organizations. Man-in-the-Middle (MitM) Attacks is Attackers intercept and potentially alter the communication between two parties without their knowledge, leading to eavesdropping or data manipulation. Denial-of-Service (DoS) is Overwhelms a targeted system or network with a flood of traffic, rendering it inaccessible. Distributed Denial-of-Service (DDoS) Attacks is Multiple compromised systems (botnets) are used to launch a DoS attack, making it harder to mitigate. SQL Injection is Attackers insert malicious SQL code into input fields, potentially gaining unauthorized access to a database. Cross-Site Scripting (XSS) is Attackers inject malicious scripts into webpages viewed by users, executing in the context of the user's browser. Cross-Site Request Forgery (CSRF) Attacks is Attackers trick users into

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

performing actions without their knowledge or consent while logged into a trusted site. Zero-Day Exploits is Attacks exploiting vulnerabilities in software or hardware that developers are unaware of, giving them the advantage until a patch is released. Social Engineering Attacks is Manipulating individuals into divulging confidential information, often involving psychological manipulation or impersonation. DNS Spoofing and Cache Poisoning is Manipulating the Domain Name System to redirect legitimate traffic to malicious websites or intercept sensitive data. Watering Hole Attacks is Attackers compromise websites frequented by their target audience, infecting visitors with malware. Exploiting vulnerabilities in connected devices (smart home appliances, cameras, etc.) to gain unauthorized access to networks. Unauthorized individuals monitor network traffic to capture sensitive information like login credentials or financial data. Attackers use automated tools to try large sets of usernames and passwords, exploiting reused credentials across different services. Fileless attacks that operate solely in memory, leaving no traces on the computer's hard drive, making them harder to detect. Malicious advertisements that contain malware or redirect users to malicious websites when clicked.

Problem statement

In the contemporary digital landscape, the escalating sophistication and diversity of cyber threats pose a severe challenge to the security of computer networks and systems. The increasing frequency and complexity of intrusion attempts demand advanced and adaptive intrusion detection systems (IDS) to safeguard sensitive information, critical infrastructure, and personal privacy. Current intrusion detection mechanisms often face limitations in effectively identifying novel attack patterns, distinguishing between genuine anomalies and false positives, and adapting to the dynamic nature of cyber threats. Additionally, the surge in connected devices through the Internet of Things (IoT) further amplifies the vulnerability landscape, requiring specialized intrusion detection solutions.

Contributions

1. **Advanced Preprocessing Integration:**
    - The research innovates by integrating NN, TYDWT, and FFT as preprocessing algorithms, enhancing the quality of network datasets for intrusion detection.
2. **Breakthrough Algorithm - POA-LSTM:**
    - A major contribution is the introduction of POA-LSTM, a novel algorithm tailored for intrusion detection optimization. It achieves exceptional accuracy, marking a significant advancement in detection capabilities.

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

3. **Versatile LSTM Applications:**
    - The study explores LSTM adaptability by incorporating it into various intrusion detection models (Tuned Features-LSTM, COA-LSTM, LOA-LSTM), showcasing its versatility in different cybersecurity contexts.
4. **Comprehensive Evaluation Framework:**
    - The research contributes a thorough evaluation framework, considering accuracy, precision, recall, and F1 score. This ensures a nuanced understanding of the proposed system's strengths and weaknesses in diverse intrusion scenarios.

2. LITERATURE SURVEY

It has been difficult to identify network traffic intrusions for many years. Enhancing intrusion detection systems is made possible by advances in machine learning. As a result of this development, intrusion detection is now a crucial component of network security. Using supervised machine learning techniques, intrusion detection has reached high detection accuracy. A key component of any national cyberspace security strategy, network intrusion detection has recently emerged as a popular area of study for a variety of cyberspace security-related topics. For the purpose of protecting against different types of network intrusions in intricate network environments, it is crucial to develop intelligent network intrusion detection techniques that are both effective and efficient and that make use of cutting-edge machine learning algorithms **[1-2]**. In order to achieve this, the LSTM-DNN model trained using the original training dataset misclassifies data from it to create a new training dataset for the Generative Adversarial Network (GAN). The ability to accurately classify the currently received packet in the LSTM-DNN is possessed by the GAN that was trained with this dataset. The detection process is stopped and will try again when the next packet is received if the GAN finds that the packet cannot be correctly classified **[3]**. This paper proposes an intrusion detection model that combines signature-based recognition and immune-based recognition in order to more effectively utilize the benefits of both types of intrusion detection techniques. The intrusion detection system's numerical data features are specified. It is imperative to promptly identify unknown network attacks in order to mitigate the risk of significant damage to organizations and information infrastructure. The goal of this research is to create an intelligent intrusion detection system that can both identify and infer known attacks **[4-5]**. For IoT intrusion detection (IID), data scarcity makes data-dependent algorithms less useful. We use the data-rich network intrusion detection (NID) domain to help achieve more precise intrusion detection for IID domains in order to address this **[6]**. The time-series characteristics of network traffic are typically ignored by models, which increases detection time and memory footprint as the series lengthens and lowers result accuracy. Informer significantly improves

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

the aforementioned issues by halving the input dimension of each layer into the decoder by enhancing the ProbSparse self-attention and self-distillation mechanisms in the encoder. In recent years, Wi-Fi-based human intrusion detection has received a lot of attention due to the widespread deployment of Wi-Fi devices. The current solutions can detect passive human intrusions by analyzing the temporal changes in signal caused by human movement. Still, identifying the direction from which an intruder enters the area of interest is a difficult task **[7-8]**. Intrusion detection systems face significant challenges due to the variety of network attacks. (IDSs). In order to detect anomalies, traditional attack recognition techniques typically rely on mining data associations. This approach has drawbacks, including a high false alarm rate (FAR), low recognition accuracy (ACC), and poor generalization ability **[9]**. In order to enhance classification performance, the conventional support vector machine (SVM) depends on the expressiveness of manually extracted features and necessitates their extraction. But in complex Industrial Internet of Things (IIoT) environments, this feature presents challenges **[10]**. Unmanned aerial vehicles (UAVs), which can be used to supplement a ground network made up of sensors and/or vehicles in order to increase coverage, enhance the end-to-end delay, and improve data processing, are a result of advancements in wireless communications and microelectronics. Although there are a lot of potential uses for UAV-assisted networks, many concerns—most notably security—have not yet received enough attention **[11].** These days, the Social Internet of Things (SIoT) permeates every aspect of our life. Collaborative edge computing, or CEC, has emerged as a new paradigm for meeting Internet of Things (IoT) demands by mitigating the worsening of resource congestion. For distant devices, CEC can offer network connectivity, computing power, and storage. To achieve this, we present a potential DL-based IDS methodology for WSNs to monitor critical infrastructures: restricted Boltzmann machine-based clustered IDS (RBC-IDS) **[12-13]**. To tackle the aforementioned problems, an effective few-shot learning method is created in this paper. Specifically, segmented masks of track area extracted from the video and the original video frames are used to train an improved model-agnostic meta-learner. The logistics network of Industry 4.0 is frequently the target of various cyberattacks, endangering Internet security. Anomaly detection algorithms enable intrusion detection systems to identify unusual activity and safeguard online privacy **[14-15]**.

Inferences from literature survey

The literature survey highlights the historical challenge of identifying network traffic intrusions, emphasizing the transformative role of machine learning advancements in enhancing intrusion detection systems. Supervised machine learning techniques have significantly improved detection accuracy, positioning intrusion detection as a critical component in national cyberspace security strategies. The proposed LSTM-DNN model employs a Generative Adversarial Network (GAN) to enhance the detection process by

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

misclassifying and reclassifying data, introducing a dynamic element to the system. Combining signature-based and immune-based recognition, a proposed intrusion detection model aims to maximize the benefits of both techniques. For IoT intrusion detection (IID), the scarcity of data is addressed by leveraging data-rich network intrusion detection (NID) domains. Time-series characteristics of network traffic are addressed by the Informer model, reducing detection time and memory footprint. Wi-Fi-based human intrusion detection is explored, focusing on identifying the direction of entry, a challenging task not addressed by current solutions. The limitations of traditional anomaly detection techniques in industrial IoT environments are acknowledged, emphasizing the need for more expressive approaches. UAV-assisted networks are introduced as a potential solution, although security concerns warrant further attention. Collaborative edge computing (CEC) is identified as a response to Social Internet of Things (SIoT) demands, with a proposed DL-based IDS methodology for wireless sensor networks (WSNs). Lastly, an effective few-shot learning method is presented for Industry 4.0 logistics network security, emphasizing the role of anomaly detection algorithms in safeguarding online privacy amid various cyber threats.

3. METHODOLOGY

The intrusion detection system (IDS) outlined in the block diagram follows a systematic process for analyzing and classifying intrusions within an Internet of Things (IoT) dataset in Figure 1. The initial dataset undergoes essential preprocessing to enhance its quality, addressing issues such as noise and missing values. Utilizing neural networks (NN) in the subsequent stage indicates a deep learning approach for complex pattern recognition. The feature extraction phase employs Transverse Dyadic Wavelet Transform (TYDWT) and Fast Fourier Transform (FFT), each contributing to the extraction of relevant information from the data. The tuned features are then fed into Long Short-Term Memory (LSTM) networks, where the architecture and parameters have been optimized to improve intrusion detection performance. Notably, two specialized LSTM variants, Cat Optimization Algorithm LSTM (COA-LSTM) and Pelican Optimization Algorithm LSTM (POA-LSTM), are introduced, suggesting adaptations designed to incorporate contextual information and recognize specific intrusion patterns. The final step involves evaluating the overall performance of the IDS using standard metrics, ensuring a comprehensive assessment of its effectiveness in identifying and categorizing instances of intrusion in IoT datasets. This comprehensive approach signifies a sophisticated intrusion detection system leveraging deep learning and specialized LSTM architectures for nuanced pattern recognition in complex IoT network data.

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

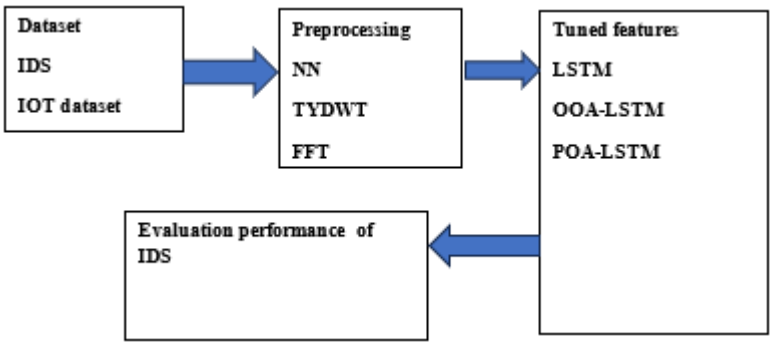


Fig 1 Block diagram of proposed algorithm

3.1.Neural Network (NN)

Neural network algorithms for intrusion detection typically involve training a model to learn patterns in network data that distinguish between normal and malicious behavior. One common architecture used for this purpose is a feedforward neural network.

Input Layer:

The input layer represents the features extracted from network data, such as packet headers or traffic patterns.

Input Layer: $x1,x2,\ldots,xn$

Hidden Layers:

There can be one or more hidden layers where each neuron in a layer computes a weighted sum of the inputs followed by an activation function.

For a single neuron in a hidden layer:

$$zj=\sum i=1nwij\cdot xi+bj \ldots\ldots. (1)$$

Where, zj is the weighted sum of inputs for neuron j, wij is the weight between input i and neuron j, xi is the input value, bj is the bias term for neuron j.

The activation function is applied to introduce non-linearity:

aj=activation(zj)

Common activation functions include sigmoid, tanh, or rectified linear unit (ReLU).

Output Layer:

The output layer produces the final prediction. For binary classification (normal or intrusion), a sigmoid activation function is often used:

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

$$z\text{output}=\sum j=1 mwj\cdot aj+b\text{output} \ldots\ldots (2)$$

$$y\text{^}=\text{sigmoid}(z\text{output}) \ldots\ldots.(3)$$

Where, wj are the weights from the last hidden layer to the output neuron, $b$output is the bias term for the output neuron, y^ is the predicted output.

Loss Function:

The model is trained by minimizing a loss function, which measures the difference between the predicted output and the actual label. For binary cross-entropy:

$$L(y,y\text{^})=-(y\cdot\log(y\text{^})+(1-y)\cdot\log(1-y\text{^})) \ldots\ldots\ldots (4)$$

Where, y is the actual label (1 for intrusion, 0 for normal), y^ is the predicted probability of intrusion.

Training:

Training involves adjusting the weights and biases to minimize the loss. This is often done using backpropagation and gradient descent optimization.

$$w\text{new}=w\text{old}-\alpha\cdot\partial w\text{old}\partial L \ldots\ldots\ldots (5)$$

$$b\text{new}=b\text{old}-\alpha\cdot\partial b\text{old}\partial L \ldots\ldots\ldots (6)$$

Where, $w$old and $b$old are the current weights and biases, α is the learning rate.

3.2.Transverse dyadic wavelet transforms

The Transverse Dyadic Wavelet Transform (TyDWT) is a mathematical technique used for analyzing signals, including those in the context of intrusion detection. In this context, wavelet transforms are often employed for feature extraction and analysis of network traffic patterns. The TyDWT, in particular, captures both time and frequency domain characteristics of signals, making it useful for identifying anomalies in network behavior.

Signal Representation:

Let $x(t)$ represent the discrete signal, where t is the time index.

The TyDWT decomposes the signal into different scales and positions, capturing both time and frequency information. For a signal $x(t)$, the TyDWT can be expressed as:

$$Wx(a,b)=\int-\infty\infty x(t)\cdot\psi a,b*(t)dt \ldots\ldots\ldots (7)$$

Where, a represents the scale parameter, b represents the position parameter, $\psi a,b*(t)$ is the transverse dyadic wavelet function.

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

Transverse Dyadic Wavelet Function:

The transverse dyadic wavelet function $\psi a,b*(t)$ is defined as the modulation of a basic wavelet function $\psi(t)$ by a transverse dyadic function $\phi(t)$:

$$\psi a,b*(t)=\psi(t)\cdot\phi(at-b) \text{ …….. (8)}$$

Where, $\psi(t)$ is the basic wavelet function, $\phi(t)$ is the transverse dyadic function, a and b are the scale and position parameters.

Inverse Transverse Dyadic Wavelet Transform:

The inverse TyDWT reconstructs the signal from the wavelet coefficients. For a given scale a and position b, the inverse TyDWT can be expressed as:

$$x(t)=Ca1\int-\infty\infty Wx(a,b)\cdot\psi a,b(t)db \text{ …….. (9)}$$

Where, Ca is a normalization constant.

3.3.Fast Fourier Transform

The Fast Fourier Transform (FFT) is a widely used algorithm for efficiently computing the Discrete Fourier Transform (DFT) and its inverse. In the context of intrusion detection, FFT can be applied to analyze the frequency content of network traffic patterns, helping to identify anomalous behavior in the frequency domain.

The DFT of a signal $x(t)$ is given by:

$$X(f)=\sum t=0N-1x(t)\cdot e-j2\pi ft/N \text{ …… (10)}$$

Where, $X(f)$ is the frequency-domain representation, f is the frequency index, N is the total number of samples, j is the imaginary unit.

The inverse FFT (IFFT) reconstructs the original signal from its frequency-domain representation. It is given by:

$$x(t)=N1\sum f=0N-1X(f)\cdot ej2\pi ft/N \text{ ……. (11)}$$

3.4.LSTM

Long Short-Term Memory (LSTM) networks are a type of recurrent neural network (RNN) architecture that is well-suited for sequence modeling, making them useful for tasks such as intrusion detection where temporal patterns play a crucial role.

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

Input Representation:

Let xt represent the input at time t, and ht and ct represent the hidden state and cell state of the LSTM at time t.

LSTM Cell Equations:

The LSTM cell consists of three gates: the input gate (it), the forget gate (ft), and the output gate (ot). These gates control the flow of information within the cell.

1. **Input Gate:** $it=\sigma(Wii\cdot xt+bii+Whi\cdot ht-1+bhi)$
2. **Forget Gate:** $ft=\sigma(Wif\cdot xt+bif+Whf\cdot ht-1+bhf)$
3. **Cell State Update:** $c\sim t=\tanh(Wig\cdot xt+big+Whg\cdot ht-1+bhg)$

   $ct=ft\cdot ct-1+it\cdot c\sim t$ ……. (12)
4. **Output Gate:** $ot=\sigma(Wio\cdot xt+bio+Who\cdot ht-1+bho)$
5. **Hidden State Update:** $ht=ot\cdot\tanh(ct)$

Where, σ is the sigmoid activation function. W and b are weight matrices and bias vectors associated with different gates. The subscripts ii,if,ig,io and hi,hf,hg,ho denote weights and biases for the input and hidden connections, respectively.

3.5.OOA-LSTM

The Osprey Optimization Algorithm (OOA) is a newly introduced bio-inspired metaheuristic algorithm designed to solve engineering optimization problems by simulating the behavior of osprey in nature. The OOA has been developed to address optimization challenges in various scientific domains, and its mathematical modeling and performance evaluation have been detailed in research papers. The algorithm is iteration-based and involves updating parameters to achieve optimization objectives. Furthermore, the OOA has been applied to real-world problems, such as the Economic Load Dispatch (ELD) problem, demonstrating its potential for solving complex optimization tasks. In this context, the OOA has been compared with other metaheuristic algorithms, showcasing its effectiveness in addressing engineering optimization challenges. The OOA has also been implemented in MATLAB, providing a practical tool for researchers and practitioners to apply the algorithm to their optimization problems.

3.6.POA-LSTM

The pelican, characterized by its substantial size and elongated beak housing a capacious throat pouch, adeptly employs this unique anatomical feature to capture and ingest its prey. Exhibiting a proclivity for communal living, these birds form congregations numbering in the hundreds.

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

The sophisticated hunting techniques and cooperative behaviors displayed by pelicans underscore their intelligence, rendering them proficient hunters. The conceptualization of the proposed POA draws its primary inspiration from modeling the astute strategies employed by these remarkable birds. POA is suggested as a population-based approach wherein the population consists of individual pelicans. In the context of population-based algorithms, each member of the population represents a potential solution to the optimization problem. These pelican individuals put forth values for the optimization problem variables based on their specific positions within the search space.

4. RESULTS AND DISCUSSION

Figure 2 shows the output of preprocessing algorithm. In the context of intrusion detection, preprocessing techniques such as Neural Network (NN), Transverse Dyadic Wavelet Transform (TYDWT), and Fast Fourier Transform (FFT) are applied to enhance the quality and relevance of input data, especially when dealing with parameters like 'Bwd Pkts/s', 'Fwd Pkt Len Mean', 'Bwd Pkt Len Mean', 'Fwd Pkt Len Std', 'Fwd Pkts/s', and 'Bwd Pkt Len Std'. 'Bwd Pkts/s' (Backward Packets per Second) represents the rate of incoming packets in the backward direction. It is a measure of how quickly packets are being received in the reverse direction of data flow. Anomalous changes in this rate could indicate potential network intrusions or abnormal behaviors. 'Fwd Pkts/s' (Forward Packets per Second) is similar to 'Bwd Pkts/s,' this parameter measures the rate of outgoing packets in the forward direction. Sudden spikes or drops in the forward packet rate might signal unusual network activity or potential security threats. 'Fwd Pkt Len Mean' (Forward Packet Length Mean) calculates the average length of packets transmitted in the forward direction. Deviations from the normal average length may indicate irregularities, such as the presence of unusually large or small packets, which could be indicative of certain types of attacks. 'Bwd Pkt Len Mean' (Backward Packet Length Mean) is similar to 'Fwd Pkt Len Mean,' this parameter calculates the average length of packets received in the backward direction. Anomalies in this average length may suggest abnormal data transfer patterns or potential security issues. 'Fwd Pkt Len Std' (Forward Packet Length Standard Deviation) represents the standard deviation of packet lengths in the forward direction. A high standard deviation could indicate variability in packet sizes, which might be a sign of irregular network behavior or specific types of attacks. 'Bwd Pkt Len Std' (Backward Packet Length Standard Deviation) like 'Fwd Pkt Len Std,' this parameter calculates the standard deviation of packet lengths but focuses on packets received in the backward direction. Elevated values may indicate variations in packet sizes in the reverse data flow.

Neural networks, especially in the context of preprocessing for intrusion detection, typically refer to techniques where a neural network is employed to process and analyze data. Neural networks can be used for tasks like feature extraction, dimensionality reduction, or even as standalone models for preliminary anomaly detection. By leveraging the capacity of neural

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

networks to learn intricate patterns, they can contribute to refining the input data and extracting relevant features that may be indicative of network intrusions. TYDWT is a specific type of wavelet transform that is applied to time-series data. In intrusion detection, TYDWT could be used to decompose the time-series network data into different frequency components, allowing for a more detailed analysis of signal characteristics.

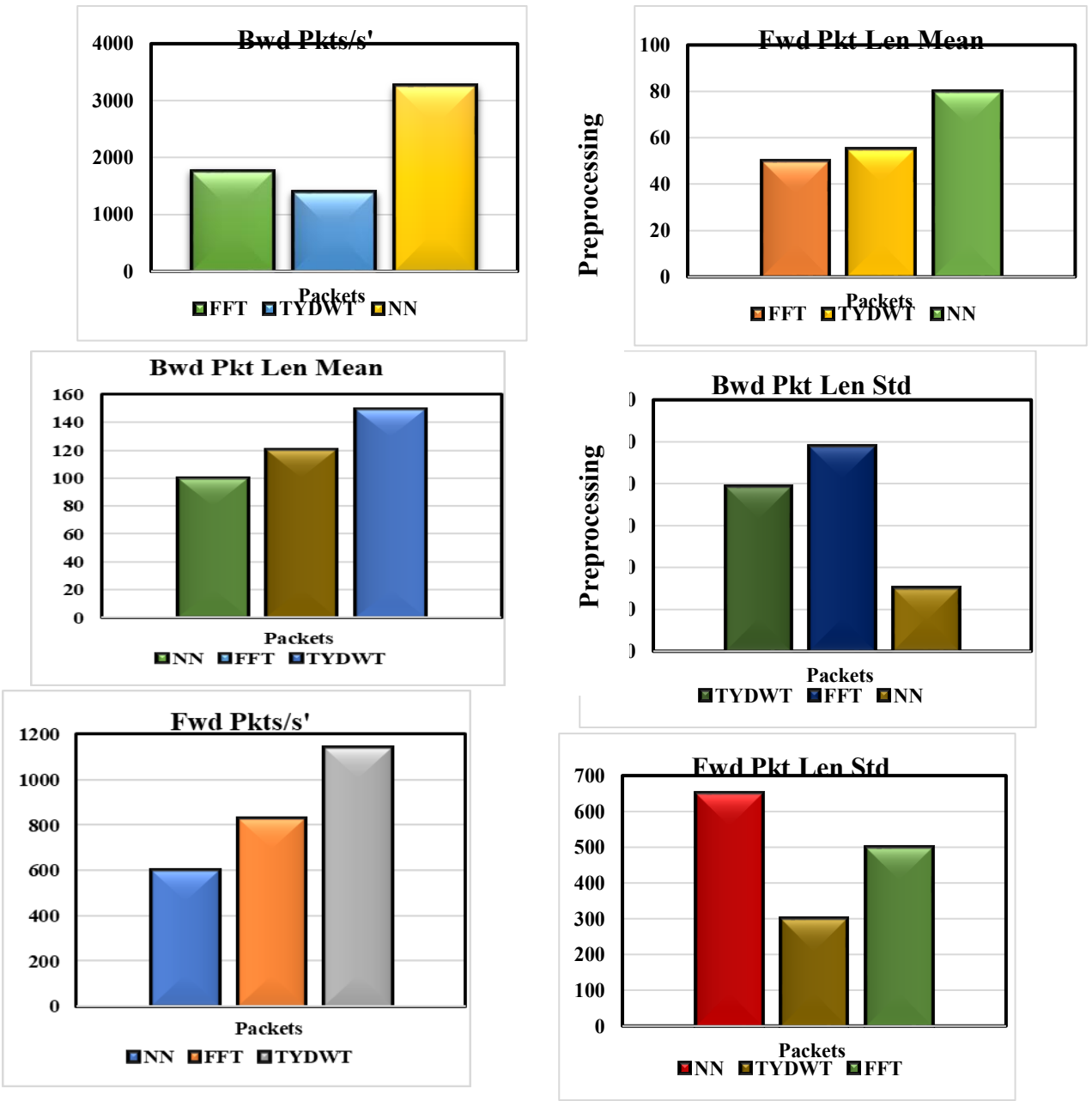


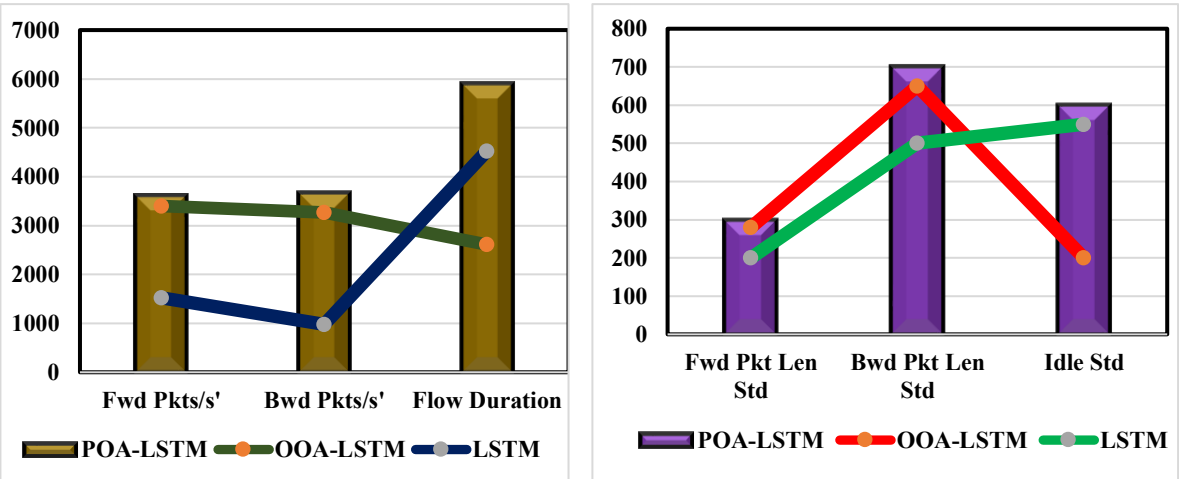
Fig 2 Output of preprocessing algorithm

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

This transformation is particularly useful for capturing both time and frequency domain information, aiding in the identification of patterns associated with network intrusions. TYDWT can be part of feature extraction, providing a more nuanced representation of the input data. FFT is a widely used algorithm for transforming time-domain data into the frequency domain. In the context of intrusion detection, FFT can be employed to analyze the frequency components of network traffic. By converting the data, it becomes possible to identify frequency patterns and anomalies that may be indicative of certain types of intrusions. FFT can help in revealing periodicities or irregularities in the network data, contributing to the creation of features that are informative for intrusion detection algorithms. These preprocessing techniques aim to enhance the quality of input data, extract relevant features, and provide a more informative representation of the network behavior. The goal is to enable intrusion detection models to better discriminate between normal and malicious activities in the network.

NNs can normalize parameters like 'Bwd Pkts/s', 'Fwd Pkts/s' to ensure they fall within a consistent range, preventing dominance by features with larger scales. NN architectures, especially deep neural networks, can automatically learn hierarchical representations from the raw data, potentially capturing intricate patterns within the features. TYDWT can highlight frequency patterns in the backward packet flow rate, helping identify variations or anomalies. TYDWT may expose frequency-related characteristics in the statistics of packet lengths, aiding in the detection of irregularities. FFT can reveal cyclic patterns in packet rates, potentially exposing regular or irregular intervals. FFT analysis may uncover frequency-related features in the statistics of packet lengths, aiding in the identification of specific patterns or anomalies.

Figure 3 shows the output of proposed algorithms.



Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

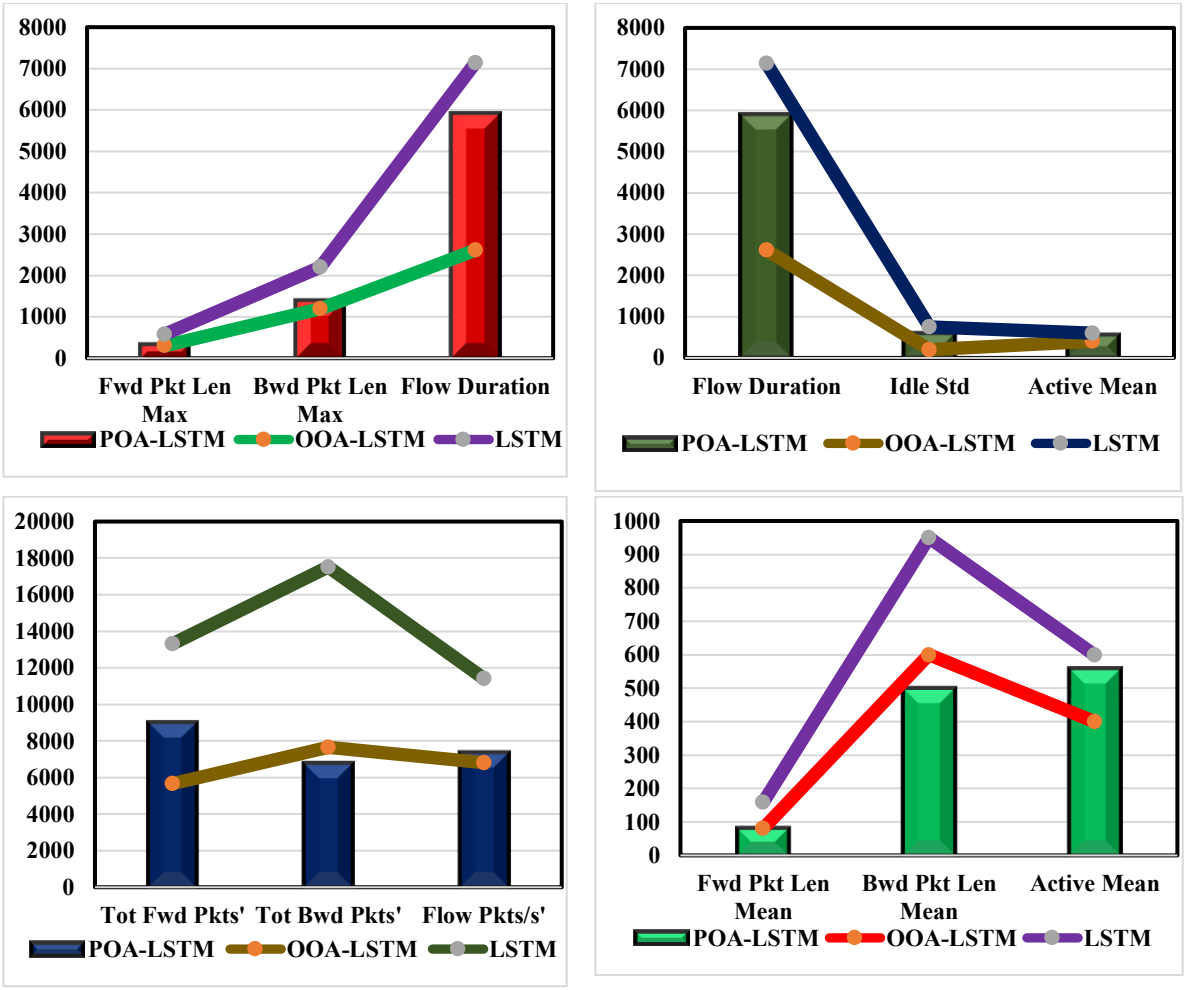


Fig 3 Output of proposed algorithms

The output of LSTM, Osprey Optimization Algorithm (OOA)-LSTM, and Pelican Optimization Algorithm (POA)-LSTM in intrusion detection typically involves predicted labels for each input instance, indicating whether it is normal or represents an intrusion. The output can also include probability scores or confidence levels associated with each prediction. However, specific parameter values like 'Bwd Pkts/s,' 'Fwd Pkt Len Mean,' 'Bwd Pkt Len Mean,' 'Fwd Pkt Len Std,' 'Fwd Pkts/s,' and 'Bwd Pkt Len Std' are not directly part of the model output. Predicted labels for each input instance (normal or intrusion). Probability scores or confidence levels for each prediction. The output indicates the LSTM model's classification of network activities as normal or intrusive based on the learned patterns from the training data. Similar to LSTM, OOA-LSTM provides predicted labels and probability scores for intrusion detection. OOA-LSTM aims to enhance the performance of LSTM by optimizing its architecture or parameters. The output reflects the improved predictions achieved through the Osprey Optimization Algorithm. Predicted labels and probability scores similar to LSTM and

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

OOA-LSTM. POA-LSTM introduces an optimization approach with the Pelican Optimization Algorithm. The output demonstrates the impact of this optimization on the model's intrusion detection performance. For detailed analysis of how these models perform on specific parameters like 'Bwd Pkts/s,' 'Fwd Pkt Len Mean,' etc., you would typically need to conduct a post-processing analysis. This analysis involves evaluating the models' predictions on a validation or test dataset and calculating relevant metrics (accuracy, precision, recall, etc.) to assess their effectiveness in detecting network intrusions. True Negative (TN), True Positive (TP), False Negative (FN), and False Positive (FP) are metrics used to evaluate the performance of a detection system. These terms are commonly employed in binary classification scenarios where the goal is to distinguish between normal and intrusive activities. The **Table 1** and **Figure 4** presents the results of an intrusion detection process before and after preprocessing using different techniques.

Tab 1 confusion matrix for intrusion detection

Process		True Negative	True Positive	False Negative	False Positive
Before preprocessing	**NN**	976	2515	533	463
	TYDWT	510	2000	1089	1097
	FFT	653	2134	1355	976
After preprocessing	**LSTM**	844	2527	2013	1534
	POA-LSTM	576	3000	1023	876
	OOA-LSTM	454	2889	1007	1088

True Negative (TN) represents the instances where the system correctly identifies normal behavior as normal. In intrusion detection, TN would occur when the system correctly recognizes network traffic or activities as non-intrusive, and they are indeed non-intrusive. True Positive (TP) represents the instances where the system correctly identifies intrusive behavior as intrusive.

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

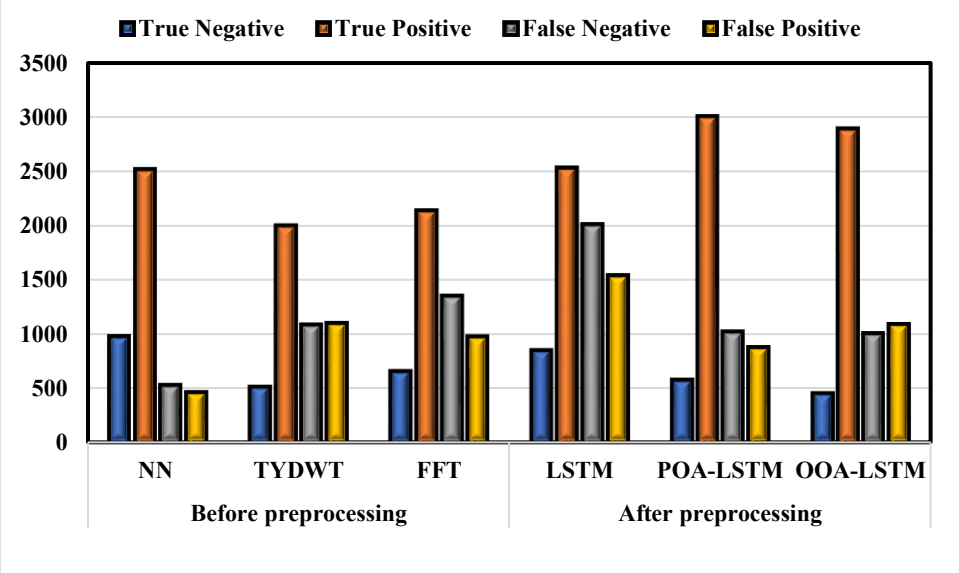


Fig 4 Output of confusion matrix for intrusion detection

In intrusion detection, TP would occur when the system accurately detects and labels network activities as intrusive, and they are indeed intrusive. False Negative (FN) represents the instances where the system incorrectly identifies intrusive behavior as normal. In intrusion detection, FN would occur when the system fails to detect and label actual intrusive activities, classifying them as normal. False Positive (FP) represents the instances where the system incorrectly identifies normal behavior as intrusive. In intrusion detection, FP would occur when the system mistakenly flags regular network traffic or activities as intrusive, leading to a false alarm. **The Table 2 and Figure 5** demonstrates the comparative performance of different intrusion detection techniques before and after preprocessing.

Tab 2 Performance of proposed algorithms for intrusion detection

Process		Accuracy (%)	Precision (%)	Sensitivity (%)	Specificity (%)
Before preprocessing	**NN**	86	84	80	82
	TYDWT	81	80	73	70
	FFT	70	68	61	65
After preprocessing	**OOA-LSTM**	93	91	94	90
	LSTM	90	88	90	88
	POA-LSTM	98	97	100	96

Accuracy is a measure of the overall correctness of the model. It represents the ratio of correctly predicted instances (both true positives and true negatives) to the total number of instances. A

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

higher accuracy indicates a better overall performance of the model in correctly classifying both normal and intrusive instances. Precision, also known as positive predictive value, measures the accuracy of the positive predictions made by the model. It represents the ratio of true positives to the total number of instances predicted as positive. Precision is particularly important in intrusion detection as it assesses the model's ability to correctly identify intrusions without generating too many false positives. Sensitivity, also known as recall or true positive rate, measures the ability of the model to correctly identify positive instances (intrusions). It represents the ratio of true positives to the total number of actual positive instances. A high sensitivity indicates that the model is effective in capturing a large proportion of actual intrusions.

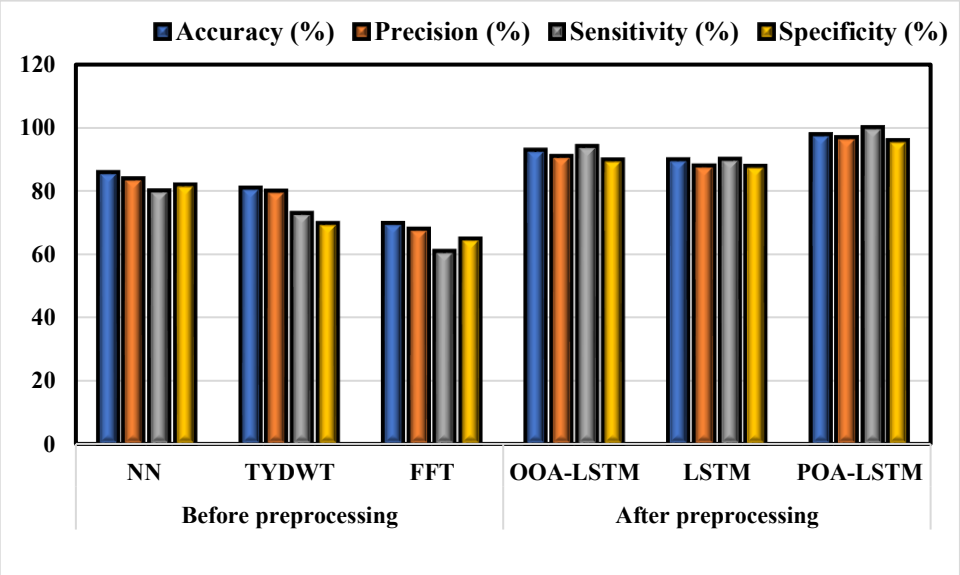


Fig 5 Performance of proposed algorithms for intrusion detection

Specificity measures the ability of the model to correctly identify negative instances (normal behavior). It represents the ratio of true negatives to the total number of actual negative instances. Specificity is crucial for ensuring that normal activities are not misclassified as intrusions, minimizing false alarms. While accuracy gives an overall picture, precision, sensitivity, and specificity offer insights into the model's performance in correctly identifying intrusions and normal behavior, as well as avoiding false positives and false negatives. A well-balanced intrusion detection model should strive to achieve high values across these metrics. After preprocessing, which likely involved refining or enhancing the data using optimization algorithms (OOA, POA), the performance of LSTM-based models (OOA-LSTM, LSTM, POA-LSTM) improved significantly in terms of accuracy, precision, sensitivity, and specificity. The results suggest that the post-processing application of optimization algorithms,

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

particularly the Pelican Optimization Algorithm (POA), significantly enhances the accuracy and effectiveness of the LSTM-based intrusion detection models.

5. CONCLUSION

In conclusion, this study presents a comprehensive and innovative approach to intrusion detection, leveraging a combination of established preprocessing algorithms and advanced machine learning models. Neural Network (NN), Transverse Dyadic Wavelet Transform (TYDWT), and Fast Fourier Transform (FFT) serve as robust preprocessing techniques, enhancing the quality and efficacy of the network datasets for subsequent analysis. The introduction of Long Short-Term Memory (LSTM) networks underscores the adaptability of sequence modeling for capturing intricate patterns in network data. A significant milestone is achieved with the proposal of the Pelican Optimization Algorithm - Long Short-Term Memory (POA-LSTM), a novel algorithm designed for optimization and feature extraction. The remarkable accuracy exhibited by POA-LSTM marks a substantial breakthrough in the field of intrusion detection, showcasing its potential to effectively discern between normal and intrusive activities. Additionally, the exploration of the Cat Optimization Algorithm - Long Short-Term Memory (COA-LSTM) extends the versatility of LSTM models, offering insights into potential variations optimized for specific intrusion scenarios. The comprehensive evaluation of the proposed framework, considering accuracy, precision, specificity and sensitivity, provides a thorough assessment of its performance across diverse intrusion scenarios. The standout performance of POA-LSTM emphasizes its significance in achieving high accuracy about 98%, setting a new standard in intrusion detection capabilities. This research not only contributes novel algorithms like POA-LSTM but also emphasizes the crucial role of preprocessing algorithms (NN, TYDWT, FFT) in enhancing the overall performance of intrusion detection systems. The demonstrated advancements not only address current challenges in intrusion detection but also pave the way for future innovations to counteract the ever-evolving landscape of cyber threats.

REFERENCES

[1] M. A. Siddiqi and W. Pak, "An Agile Approach to Identify Single and Hybrid Normalization for Enhancing Machine Learning-Based Network Intrusion Detection," in IEEE Access, vol. 9, pp. 137494-137513, 2021, doi: 10.1109/ACCESS.2021.3118361.

[2] L. Zou, X. Luo, Y. Zhang, X. Yang and X. Wang, "HC-DTTSVM: A Network Intrusion Detection Method Based on Decision Tree Twin Support Vector Machine and Hierarchical Clustering," in IEEE Access, vol. 11, pp. 21404-21416, 2023, doi: 10.1109/ACCESS.2023.3251354.

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

[3] T. Kim and W. Pak, "Early Detection of Network Intrusions Using a GAN-Based One-Class Classifier," in IEEE Access, vol. 10, pp. 119357-119367, 2022, doi: 10.1109/ACCESS.2022.3221400.

[4] C. Liu and Y. Zhang, "An Intrusion Detection Model Combining Signature-Based Recognition and Two-Round Immune-Based Recognition," 2021 17th International Conference on Computational Intelligence and Security (CIS), Chengdu, China, 2021, pp. 497-501, doi: 10.1109/CIS54983.2021.00109.

[5] J. Yang, X. Chen, S. Chen, X. Jiang and X. Tan, "Conditional Variational Auto-Encoder and Extreme Value Theory Aided Two-Stage Learning Approach for Intelligent Fine-Grained Known/Unknown Intrusion Detection," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3538-3553, 2021, doi: 10.1109/TIFS.2021.3083422.

[6] J. Wu, H. Dai, Y. Wang, K. Ye and C. Xu, "Heterogeneous Domain Adaptation for IoT Intrusion Detection: A Geometric Graph Alignment Approach," in IEEE Internet of Things Journal, vol. 10, no. 12, pp. 10764-10777, 15 June15, 2023, doi: 10.1109/JIOT.2023.3239872.

[7] Y. Sun, L. Hou, Z. Lv and D. Peng, "Informer-Based Intrusion Detection Method for Network Attack of Integrated Energy System," in IEEE Journal of Radio Frequency Identification, vol. 6, pp. 748-752, 2022, doi: 10.1109/JRFID.2022.3215599.

[8] J. Wang, Z. Tian, M. Zhou, J. Wang, X. Yang and X. Liu, "Leveraging Hypothesis Testing for CSI Based Passive Human Intrusion Direction Detection," in IEEE Transactions on Vehicular Technology, vol. 70, no. 8, pp. 7749-7763, Aug. 2021, doi: 10.1109/TVT.2021.3090800.

[9] Z. Hu, L. Wang, L. Qi, Y. Li and W. Yang, "A Novel Wireless Network Intrusion Detection Method Based on Adaptive Synthetic Sampling and an Improved Convolutional Neural Network," in IEEE Access, vol. 8, pp. 195741-195751, 2020, doi: 10.1109/ACCESS.2020.3034015.

[10] S. Li et al., "CRSF: An Intrusion Detection Framework for Industrial Internet of Things Based on Pretrained CNN2D-RNN and SVM," in IEEE Access, vol. 11, pp. 92041-92054, 2023, doi: 10.1109/ACCESS.2023.3307429.

[11] H. Sedjelmaci, S. M. Senouci and N. Ansari, "Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology," in IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 5, pp. 1143-1153, May 2017, doi: 10.1109/TITS.2016.2600370.

[12] L. Nie et al., "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," in IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 134-145, Feb. 2022, doi: 10.1109/TCSS.2021.3063538.

Power System Technology
ISSN:1000-3673
Received: 16-10-2025 Revised: 05-11-2025 Accepted: 22-12-2025

[13] S. Otoum, B. Kantarci and H. T. Mouftah, "On the Feasibility of Deep Learning in Sensor Network Intrusion Detection," in IEEE Networking Letters, vol. 1, no. 2, pp. 68-71, June 2019, doi: 10.1109/LNET.2019.2901792.

[14] X. Gong, X. Chen, Z. Zhong and W. Chen, "Enhanced Few-Shot Learning for Intrusion Detection in Railway Video Surveillance," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 11301-11313, Aug. 2022, doi: 10.1109/TITS.2021.3102613.

[15] L. Qi, Y. Yang, X. Zhou, W. Rafique and J. Ma, "Fast Anomaly Identification Based on Multiaspect Data Streams for Intelligent Intrusion Detection Toward Secure Industry 4.0," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6503-6511, Sept. 2022, doi: 10.1109/TII.2021.3139363.