(ISSN: 0973-7049(P))

The Bioscan AN INTERNATIONAL QUARTERLY JOURNAL OF LIFE SCIENCES 21(3): S.I (3), 312-337, 2026 www.thebioscan.com

Adaptive Whale Optimized Neural Intelligence for Cyber Attack Detection in Industrial IOT Environments

N. RIGANA FATHIMA[1], Dr. D. MURUGAN[2]

* 1. Research scholar (Reg no: 23114012282032), Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli-12, Tamil Nadu, India

E-Mail: rigisharukh@gmail.com

2*. Professor, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli-12, Tamil Nadu, India

E-Mail: dmurugan@msuniv.ac.in

DOI: https://doi.org/10.63001/tbs.2026.v21.i03.S.I(3).pp312-337

KEYWORDS

Cybersecurity, Cyber-Physical Systems, Industrial Internet of Things, Industrial Attack, Intrusion Detection Systems, Adaptive Whale-Optimized Neural Intelligence, Machine Learning, Whale Optimization Algorithm, Artificial Neural Network, CIC-IIoT-2025 Dataset.

Article Info

Received: 09.05.2026

Accepted: 21.06.2026

Published:16.07.2026

Abstract

Important cyber-physical systems now have a much larger attack surface due to the rapid growth of Industrial Internet of Things (IIoT) infrastructures, making them vulnerable to sophisticated and constantly changing cyberthreats. High-dimensional traffic data, class imbalance, and changing attack patterns that are typical of IIoT contexts are common problems for traditional intrusion detection systems (IDS). To address these issues, this research presents an Adaptive Whale-Optimized Neural Intelligence (AWONI) model designed to identify cyberattacks in IIoT networks with accuracy and efficiency The Whale Optimization Algorithm (WOA) and an Artificial Neural Network (ANN) are used in the proposed technique to enable intelligent feature selection and optimize classification. While the ANN classifier successfully models complicated non-linear connections for multi-class attack detection, WOA is used to discover the most important characteristics within large-scale IIoT traffic data, reducing dimensionality and boosting leaming efficiency. The CIC-IIoT-2025 dataset, which includes a range of real-world industrial attack situations and typical traffic patterns, is used to evaluate the architecture. According to experimental data, the proposed model outperforms conventional machine learning (ML) and Deep Learning (DL) techniques and non-optimized neural approaches in terms of detection accuracy, false alarm rates, and computing efficiency. To promote the development of robust and intelligent industrial cybersecurity solutions, the suggested framework's adaptive, nature-inspired architecture makes it ideal for implementation in real-time and resource-constrained IIoT security situations.

1. Introduction

The fast growth of Internet usage and online services had a significant impact on cybersecurity across critical sectors, such as healthcare, education, banking, government, and military agencies. These elements have produced the perfect environment for more complex malware attacks. Viruses, worms, ransomware, and Trojan horses are examples of malevolent software. It breaches secure data and directly damages systems. The healthcare and banking sectors, which are often targeted due to the high value of their personal information [1], suffer significant risks of financial theft and

privacy violations, while educational institutions are vulnerable to interruptions due to their reliance on web-based services [2]. Furthermore, constrained model generalization and inadequate feature selection may further diminish detection efficiency. It is particularly troubling since most current optimization algorithms employ a single strategy, neglecting to achieve a balance between local refining and global exploration. Consequently, models often exhibit inadequate resolution rates or get ensnared in local optima. These constraints complicate the fulfilment of real-time demands in loT systems, since they diminish detection accuracy and may lead to considerable computational overhead [3]. Data-driven detection methodologies have emerged with the advancement of ML and DL technology, demonstrating particular advantages in handling extensive datasets and unrecognized attack patterns [4]. Nonetheless, existing ML-driven intrusion detection methods in loT environments still face challenges, including illogical feature selection, variable classifier performance, and protracted training durations [5].

The effectiveness of metaheuristic algorithms has significantly increased thanks to artificial intelligence (AI) approaches, particularly ML and DL. To improve the search strategies used by metaheuristics, machine learning algorithms analyze large datasets to find patterns and connections. For example, metaheuristic algorithms may be guided toward more optimal sites using machine learning models that identify favorable spots within the search space. Deep learning offers improved insights and makes it easier to create complex and flexible optimization techniques because of its capacity to handle complex, high-dimensional data. By incorporating Al, metaheuristics become more sophisticated and flexible as they continuously improve their search method, which makes them particularly well-suited to the intricate requirements of cybersecurity optimization of networks.

To automate and enable real-time decision-making in vital industrial sectors like automated production, renewable energy, healthcare, and transportation, the IIoT is a revolutionary framework that combines sensing, communication, and advanced control technologies, The IIoT connects many networks to improve operational effectiveness, productivity, and system reliability. Significant economic losses and safety hazards could occur as a consequence of various cybersecurity threats targeting industrial infrastructures due to the increased connectivity and data exchange. These threats include denial-of-service attacks, manipulating data, illegal entry, and advanced persistent threats.

Due to the ever-changing nature of network traffic, increased data dimensionality, and

evolving attack methods, traditional security techniques and IDS based on signatures are inadequate for modern IIoT contexts. In addition, real-time and accurate threat detection is a major challenge for industrial networks because of the frequent severe latency and resource constraints under which these networks operate. Therefore, it is critical to safeguard IIoT settings using smart and adaptive security systems that can comprehend complex traffic patterns

The detection of cyber threats has been greatly improved by recent advances in Al and MI., which have made ML feature extraction and the detection of anomalies much easier. When given large amounts of data on network traffic, ANNs do a good job of representing non-linear interactions. In the presence of noisy and imbalanced IIoT data, their performance is highly dependent on optimizing parameters and selecting suitable features.

More and more people are looking to metaheuristic optimization algorithms that are based on natural behaviors to solve these problems. A powerful global search tool with fast convergence for complex optimization problems is the WOA, which is based on the bubble-net hunting strategy used by humpback whales, When WOA is used with ANN models, feature selection, computational cost, and classification accuracy are all improved.

1.1 Motivation

This research was motivated by these results to design a system that utilizes AWONI architecture to effectively identify cyber assaults in IoT environments. It is possible to reliably identify multi-class assaults using an ANN classifier, and the strategy that has been described makes use of WOA to choose the most appropriate feature subsets and alter the default settings of the neural network. For the purpose of determining whether or not the architecture is effective, the CIC-IIoT-2025 dataset is used. This dataset is representative of actual industrial network communications and includes a number of different attack scenarios. According to the results of the experiments, the model that was proposed is an excellent choice for ongoing IoT security applications. This is because, in comparison to classic machine learning and standalone neural approaches, it provides greater detection accuracy, dependability, and efficiency.

1.2 Contributions

- This paper introduces an innovative methodology for adaptive cyber threat identification inside Industrial IoT environments by integrating the Whale Optimization Algorithm (WOA) with an Artificial Neural Network's (ANN)
- The effective use of WOA to choose the most discriminant subsets of characteristics and optimally tune ANN

parameters reduces the number of dimensions in the data, reduces noise, and improves model generalization

- The recommended method lets you find threats in a more detailed way than just putting them into two groups, and it can find and classify different types of cyber attacks in IIoT networks appropriately.
- To demonstrate that the framework can effectively handle high-dimensional, imbalanced, and inconsistent industrial network activity via comprehensive experiments conducted on the CIC-IIoT-2025 dataset.
- According to experimental results, the proposed WOA-ANN technique is well-suited for real-time IIoT security execution since it is more accurate, more resilient, and more efficient than classical machine leaming and individual neural models.
- AWONI is designed to enhance detection accuracy, quickly adapt to new malware signatures, and work well with high-dimensional, imbalanced datasets that are common in cybersecurity. It also works well with a wide range of malware.
- By scaling to enormous datasets and balancing different objectives, such as detection rate vs. false positives, the method makes the system work better.
- This study presents a novel methodology that integrates concepts from evolutionary computation and modern Al techniques AWONI. When used together, provide a powerful tool that can rapidly find the best answers, which cuts down on training time and boosts performance.

2. Related Works.

2.1 Al-Powered Security Monitoring in IIoT and IoT

To provide a unified conceptual framework and academic agenda for Al-augmented Intrusion Detection Systems inside Internet of Things environments. Their study meticulously analyzed supervised, unsupervised, and hybrid Al models, highlighting challenges such as diverse traffic patterns, limited explainability, dataset imbalance, and insufficient real-time adaptation. The methodology provides strong theoretical direction but does not develop or assess an appropriate detection model for industrial datasets, hence neglecting practical implementation issues [6].

It offered a comprehensive systematic analysis of ML and DL techniques for identifying network intrusions. The study analyzed traditional machine learning classifiers, convolutional neural networks (CNNs),

recurrent neural networks (RNNs), and hybrid models, concluding that dependence on features and static leaming approaches impede efficacy against evolving cyber threats. The work is fundamental but lacks metaheuristic optimization and adaptive intelligence, which are crucial for modern IoT security [7].

2.2 Hypothetical Optimization and Swarm Artificial Intelligence for Cybersecurity

It introduced an ML system tailored for swarms, aimed at identifying cyber threats. Utilizing swarm intelligence to adjust the classifier's parameters, the model attained enhanced detection accuracy while concurrently mimimizing false positives. The methodology relied on conventional ML classifiers and excluded deep neural structures or temporal traffic learning, hence limiting its scalability to enormous Information and Internet of Things datasets [8]

An Adjustable Boundary Whale Optimization Algorithm (ABWOA) was developed for constructing large-scale digital twin networks. The adaptive boundary technique improved both convergence stability and search variety. The study did not apply ABWOA to malware detection or cybersecurity, so its security potential was not explored [9]. Although the research was very effective in addressing optimization difficulties, it did not implement its findings in these domains.

A Lévy Flight-driven Walrus Optimization approach was developed to facilitate efficient work scheduling in IoT systems. The exploration was enhanced, and the algorithm circumvented attaining a local optimum. Conversely, the focus remained on managing resources rather than security, with less attention given to the potential for attack detection [10].

2.3 Whale Optimization and Hybrid DL Systems for Detecting Intrusions

A multiple-target Markov-enhanced adaptable whale optimization framework was introduced for binary and multi-class malware classification. The addition of Markov chains made state transition learning better, and whale optimization made classifier tuning better. The methodology focused mostly on examples of malware and didn't take into consideration real-time IIoT data streams, even though it worked very well [11].

The goal of performing cybersecurity assessments in IIoT-enabled smart manufacturing systems introduced an intelligent Whale Optimization Algorithm-Backpropagation (IWOA-BP) artificial neural network. The hybrid model improved both the velocity of development and the reliability of

classification. On the other hand, it wasn't very good at defending itself against dynamic cyber assaults since it just had static visualizations of features and no modeling of attacks over time [12].

The objective is to create a hybrid structure for WOA and deep learning that uses a Trust-Index method to find attacks on the Internet of Things. The trust-aware learning improved detection reliability, but the extra trust calculation made it much more expensive to run, which made it hard to use in IIoT nodes with very few resources [13].

It used VGG-16 with Whale Fisher Mantis Optimization (WFMO) to find cyberattacks on smart griés. Even though deep feature extraction improved accuracy, the heavy CNN architecture caused a lot of delay and energy use, which is not good for real-time industrial contexts [14].

The goal of the suggestion is to create a better whale optimization-aided neural network that can detect cyber threats. Even though optimization improved classification accuracy, the study did not use feature consolidation or adaptive learning, resulting in issues related to duplicate data and adaptability [15].

It created an ensemble DL-IDS by using an improved version of the Beluga Whale Optimization algorithm (BWOA). The ensemble was better at detecting things, but it couldn't be used in the actual world since the model was becoming more complicated and took a lot of time to train [16].

2.4 IDS for IoT Based on Deep Learning

For Internet of Things cloud settings, it offered an Efficient Net-based IDS that was made better by a strategy for optimizing football team training Even while Efficient Net was able to cut down on the number of parameters it needed and improve its accuracy, the algorithm was mostly focused on attacks on the cloud layer and didn't pay much attention to IIOT problems at the edge level [17].

To find assaults on the Internet of Things, you need to build a single learning system that uses different machine learning classifiers. The hybrid method improved detection accuracy, but it had trouble with datasets that weren't balanced and attack patterns that changed over time [18].

Evolution learning was used for the first time to create adaptive neural networks for cybersecurity. The model demonstrated the capacity to address new dangers, nonetheless, it experienced inconsistent convergence and substantial training expenses when used with extensive datasets [19]

As a framework for detecting intrusions in the

loT, a hybrid optimization-CNN framework is shown. The method's effectiveness on sequential traffic data was diminished due to the lack of temporal dependency modeling [20], but spatial feature prediction was efficient.

To merge the fuzzy C-means cluster alongside the growth whale optimization strategy, respectively. The reliance on fuzzy rules constrained the ability to generalize across various IIoT networks [21], even if the use of fuzzy rules enhanced clustering accuracy.

2.5 New Trends and Modern Paradigms.

The purpose of this study is to investigate Al systems for intelligent medical care that are founded on collaboration and leaming. In spite of the fact that the design safeguarded privacy, it also increased communication latency and made the equipment more susceptible to poisoning attacks, which rendered it less suitable for IIoT intrusion detection systems [23].

The proposed unsupervised IDS made use of autoencoders based on convolution and a single-class support vector machine (SVM). Despite the fact that the strategy was effective for attacks that were unknown, it was unable to differentiate between the various kinds of assaults [24].

It developed a trustworthy artificial intelligence system that is capable of identifying intrusions in real-time inside the IIoT. However, trust-awareness also made systems more sophisticated and delayed operations [25]. Although it made systems more dependable, it also led to them being more costly.

2.6 Intelligent Al and Metaheuristics for IoT Intrusion Detection

A cybersecurity strategy for loT networks that uses artificial intelligence by combining self-attention-based deep learning with metaheuristic optimization methods. The self-attention mechanism helps the model find long-range dependencies and complicated connections in loT traffic flows, which makes it far better at finding coordinated and sophisticated cyber-attacks. Metaheuristic methods are used to improve model parameters and feature selection, hence improving classification accuracy. Nonetheless, the research inadequately tackles computational overhead and real-time viability, which continue to be significant obstacles for extensive and resource-Limited industrial IoT implementations [26].

A Bayesian-based optimal transfer learning approach for finding cyber attacks in IoT-assisted systems that don't have a lot of resources. The suggested method uses Bayesian optimization to fine-tune hyperparameters and

transfer leaming to speed up training and cut down on the need for huge labeled datasets. This method makes it easier to find things and more accurate in places when space is limited. The model works well, but it depends a lot on pre-trained deep architectures, which may use up a lot of memory and make it harder to react to new attack patterns in IoT ecosystems that change quickly [27].

To propose an unsupervised intrusion detection method that integrates convolutional autoencoders with a one-class support vector machine. The convolutional autoencoder learns small representations of typical network activity, while the one-class SVM finds unusual deviations. This makes the method good for finding unknown and zero-day attacks. The approach works well for finding anomalies, but it can only do binary classification and can't do extensive multi-class attack identification, which is important for managing IoT security as a whole [28]

To concentrate on enhancing the efficacy of machine learning-based intrusion detection systems in scenarios characterized by unbalanced data, a prevalent challenge in real-world IoT datasets. The research used data balancing methods and refined machine learning classifiers to improve the identification of minority-class attacks. The findings show that the strategy improves recall and F1-score for infrequent attack classes, but it doesn't use adaptive or evolutionary optimization processes, which makes it less strong against cyber threats that change all the time [29].

To examine several machine learning methodologies for malware intrusion detection in Android-based IoT devices. The suggested approaches effectively detect harmful activity in mobile and IoT-integrated contexts by extracting application-level information. But the system can't find polymorphic and runtime-based malware since it only looks at static features, and the method's scalability to big industrial IoT infrastructures isn't completely addressed [30].

An adaptive deep neural network model to make demand-side management in IoT-enabled smart grid systems safer. The model changes automatically to keep up with changes in low people use energy and communicate, which makes it better at finding intrusions in smart grid situations. However, the lack of feature selection and optimization methodologies leads to increased computing complexity, thus restricting its suitability for real-time, large-scale industrial IoT security applications [31].

2.7 Deep Learning based IDS

An intrusion detection framework based on deep learning that has been improved for cybersecurity-driven industrial loT systems utilizing the Leagues Championship Algorithm (LCA). Adding LCA makes it easier to choose features and tune hyperperameters, which leads to better detection accuracy and fewer false alarms. Their method works well with high-dimensional IIoT traffic data and does well against many types of cyberattacks. The model's reliance on population-based optimization adds computing complexity, which might affect real-time implementation in industrial settings where latency is important [32].

An adaptive Al framework for industrial IoT security that can be trusted to detect intrusions in real time. By changing its learning process in reaction to new attack behaviors, the system puts a lot of stress on being explainable, adaptable, and trustworthy. The results of the experiments suggest that the system is better able to withstand zero-day and stealth assaults. The framework's strengths lie in adaptive learning and trust modeling, but it doesn't do much to look into metaheuristic-based optimization techniques for improving feature representation and classifier performance [33].

To investigate the use of machine learning approaches for providing services driven by optical network traffic, which indirectly aids in intrusion detection via the analysis of anomalous traffic patterns in high-speed networks. Their research shows that machine learning models can accurately categorize traffic patterns and improve the use of network resources. The study focuses on network performance and provisioning instead of explicitly classifying cyber-attacks, which makes it less useful for full-fledged industrial IoT intrusion detection systems [34].

To examine deep learning-based methodologies for detecting Trojan horse assaults inside cybersecurity frameworks. The research utilizes sophisticated neural architectures to discern intricate malware patterns, attaining elevated detection accuracy for Trojan-based invasions. The method works well for malware-focused situations, but it is attack-specific and can't be used in industrial IoT settings where there are many different types of attacks happening at once [35].

3. Methods and Techniques

Figure 1 displays the proposed Adaptive Whale-Optimized Neural Intelligence (AWONT) framework for identifying cyberattacks in Industrial Internet of Things (IoT) environments integrates sophisticated data-driven learning with metaheuristic optimization to address the challenges posed by high-dimensional, dynamic, and imbalanced industrial network traffic. Initially, raw IIoT traffic data undergoes

extensive preprocessing, including noise reduction, handling missing values, normalization, and encoding of categorical information. This ensures data consistency and sustained learning. Subsequently, feature extraction is performed to get the temporal, numerical, and protocol-level attributes of industrial communication flows. The Whale Optimization Algorithm (WOA) serves as an adaptive method for feature selection and hyperparameter optimization, emulating the bubble-net hunting actions performed by humpback whales to efficiently navigate and use the search space. This enhances feature relevance and reduces redundancy.

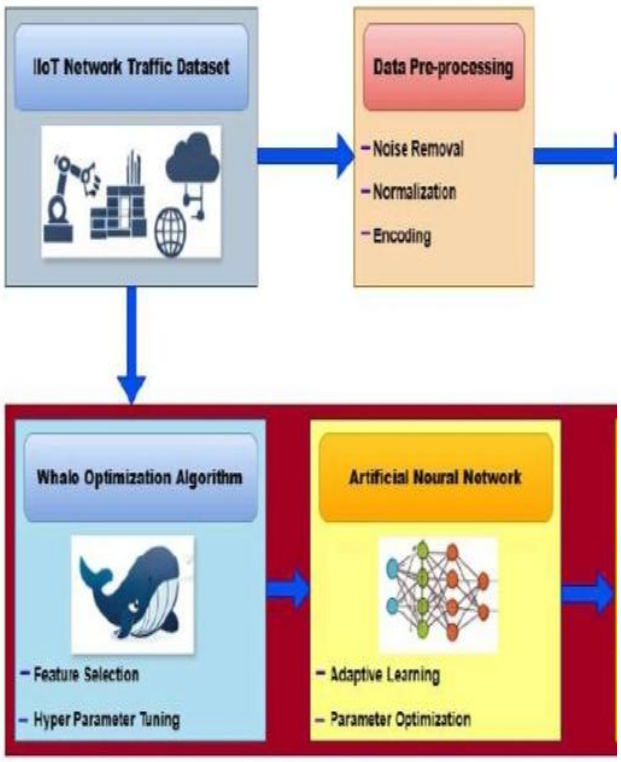

Figure 1: Proposed System Architecture

An artificial intelligence model, often adaptive Artificial Neural Network (ANN) or deep neural architecture, learns complex non-linear attack patterns in IIoT traffic by using the optimum subset of features as input. The framework's adaptability enables the neural model to modify its weights and decision thresholds in real time in response to changes in cyber-attack behaviors. WOA optimizes critical brain parameters such as the learning rate, the number of hidden neurons, and the activation functions. This accelerates model convergence and enhances classification accuracy. The last phase of categorization distinguishes between standard and multiple assault classifications in real time. This enables the identification of both recognized and emerging dangers. The integration of adaptive neural intelligence with whale-based optimization enables the suggested framework to attain elevated detection accuracy, reduced false positives, and enhanced generalization. This makes it an optimal selection for safeguarding industrial IoT ecosystems characterized by constrained resources and a diverse array of devices.

3.1 IIoT Network Traffic Dataset

The proposed AWONI-IDS utilizes the CIC-IIoT-2025 dataset. It contains authentic IIoT network traffic collected from various industrial environments, including both benign and

malicious entities. The dataset encompasses diverse communication behaviors shown by sensors, actuators, controllers, and edge devices in both normal and attack scenarios. This is relevant to both binary and multi-class classification tasks since it encompasses several attack methods, such as denial-of-service, probing, brute force, and malware-based assaults. The dataset demonstrates features indicative of genuine IIoT networks, including high dimensionality, class imbalance, and temporal variations. The increased processing complexity and decreased detection accuracy resulting from these characteristics pose significant challenges for conventional intrusion detection systems. We guarantee the model's performance is robust, scalable, and appropriate for real-time industrial security applications by assessing the suggested ATFC-Net in realistic and challenging scenarios using CIC-IIoT-2025. Engineered and implemented a functioning IIoT testbed using a diverse array of industrial sensors, IoT devices, and complementary network architecture. Transmitted network traffic and synchronized time-series sensor data for a thorough security investigation. Researchers documented a range of authentic danger situations by conducting and filming 50 distinct attack types across seven categories. Formulated and evaluated a novel methodology for feature selection with several aims, this technique enhances detection accuracy while reducing resource use. Established a standard for the classification and detection of cyberattacks using machine learning and deep learning methodologies in real-time.

3.2 Data Preprocessing

In the proposed framework, data pre-processing is essential for guaranteeing accurate and robust IDS using the CIC-IIoT-2025 dataset. The raw IIoT network data gathered in CIC-IIoT-2025 comprises diverse characteristics, noisy entries, absent values, and categorical qualities that may adversely affect learning performance if not addressed. Consequently, a first data cleansing process is implemented to eliminate duplicate flows, faulty entries, and extraneous characteristics, thereby maintaining consistency within extensive industrial traffic data. Subsequently, missing value management is executed using statistical imputation or secure default substitution to avert biased leaming CIC-IIoT-2025 incorporates protocol-level and service-based category fields, necessitating the use of label encoding or one-hot encoding to convert symbolic values into numerical formats appropriate for neural processing. Normalization by Min-Max or Z-score scaling is used to mitigate scale variance in traffic parameters, including packet size, flow length, and byte rate, facilitating accelerated convergence and steady gradient updates in the adaptive neural model. This organized pre-processing pipeline improves feature uniformity, decreases computational

complexity, and offers an optimized input space for the Whale Optimization Algorithm, thereby enhancing classification accuracy and resilience against intricate and evolving cyber-attacks in industrial IoT settings.

Normalization Equation (Min-Max Scaling):

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}}$$

Mir-Max normalization is a feature scaling method used to convert numerical input into a predetermined range, usually [0,1], which is crucial for robust and effective training of neural networks. This approach involves rescaling each feature value by removing the lowest value of the feature and dividing by the range, which is the difference between its maximum and minimum values. This guarantees that all characteristics contribute uniformly to the leaming process, avoiding attributes with greater numeric ranges (such as packet size or flow length in CIC-ΠoT-2025) from overshadowing the model's optimization. The proposed Adaptive Whale-Optimized Neural Intelligence framework utilizes Min-Max scaling to enhance gradient convergence, bolster classifier stability, and facilitate effective feature optimization through the Whale Optimization Algorithm, resulting in improved intrusion detection accuracy in industrial IoT environments.

3.3 Feature Extraction.

The proposed Adaptive Whale-Optimized Neural Intelligence (AWONI) framework incorporates Dynamic Adaptive Feature Extraction (DAFE) to identify distinguishing features of IIoT network traffic from the CIC-IIoT-2025 dataset, while accommodating changing assault patterns. In contrast to static feature extraction, the dynamic method persistently modifies feature significance in response to traffic patterns, attack severity, and temporal fluctuations in industrial networks.

Statistical parameters, including mean packet size, flow length, variance, entropy, and byte rates, are first extracted to characterize traffic distribution and identify aberrant departures. These characteristics facilitate the differentiation of standard operating traffic from attack patterns such as DDoS or brute-force efforts. Subsequently, temporal attributes are calculated dynamically using sliding windows, including inter-arrival time, burst rate, session length. and time-based packet frequency. This temporal modeling allows the system to identify slow-rate and covert assaults often seen in industrial loT settings. Moreover, protocol-level attributes like TCP flag counts, protocol utilization ratios, and service access frequency are retrieved to identify protocol abuse and illegal access behavior.

The adaptive characteristic of the feature extraction method is attained by persistently revising feature significance ratings based on input from the Whale Optimization Algorithm (WOA) and the performance of the neural classifier. Irrelevant or redundant characteristics are eliminated, while highly discriminative features are enhanced, leading to a concise and streamlined feature set. This adaptive mechanism promotes generalization, minimizes processing demands, and improves real-time cyber-attack detection accuracy, making the system resilient to both known and zero-day assaults in industrial IoT settings.

Mean and Variance Equations:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i \quad \sigma^2 = \frac{1}{N}\sum_{i=1}^{N} (x_i - \mu)^2$$

The provided equations denote statistical feature extraction often used in cyber-attack detection systems. The first equation delineates the mean (μ), which computes the average value of a characteristic over N samples. It encapsulates the fundamental trend of network traffic characteristics, including packet size, flow time, and byte count, facilitating the modeling of typical traffic behavior. The second equation delineates the variance (σ^2), which quantifies the extent to which feature values diverge from the mean. It indicates the dispersion or variety in traffic patterns. Elevated variance often signifies a typical or attack-associated conduct. Mean and variance together serve as concise statistical variables that encapsulate IIoT traffic characteristics, reduce data dimensionality, and enhance the learning effectiveness of the Adaptive Whale-Optimized Neural Intelligence model for precise cyber-attack detection.

3.4 Whale Optimization Algorithm

The proposed Whale Optimization Algorithm (WOA) serves as an intelligent optimization layer to augment the neural network's leaming potential. The system diagram demonstrates that WOA emulates the bubble-net hunting technique of humpback whales, facilitating effective exploration and exploitation of the high-dimensional IIoT feature space. Following data pretreatment and adaptive feature extraction, WOA is used to enhance essential neural parameters, including weights, biases, learning rate, and feature selection masks. The encircling prey mechanism facilitates the model's convergence to optimum solutions that depict attack and normal patterns, whilst spiral updating enhances detailed exploitation of promising solutions. The stochastic search behavior guarantees variation and prevents local minima, which is essential for identifying intricate and dynamic cyber-attacks in Industrial IoT networks. The integration of WOA with

neural intelligence enhances detection accuracy, minimizes false alarms, and accelerates convergence in dynamic assault situations. Table 1 displays the pseudocode for WOA.

Table 1: WOA Pseudocode

Input: IIoT dataset D
Output: Optimized neural model for attack detection
Step 1. Initialize whale population Wi (i= 1,2, ….N)
Step 2. Initialize neural network parameters (weights, biases)
Step 3. Preprocess dataset D (cleaning, normalization)
Step 4. Extract adaptive statistical and dynamic features
Step 5. Define fitness function:
Fitness = Classification Accuracy- False Alarm Rate
Step 6 While (t<MaxIterations):
For each whale Wi:
a. Update coefficient vectors A and C
b. If|A|<1:
//Exploitation: Encircling prey
Update Wi toward best whale Wbest
Else:
//Exploration: Random search
Select random whale Wr and update Wi
c. Apply spiral position update (bubble-net attack)
d. Update neural network parameters using Wi
e. Evaluate fitness using validation data
Update best solution Wbest
t= t+1
Step 7. Train the final neural network using optimized parameters
Step 8. Classify IIoT traffic as Normal or Attack
Step 9. Return trained detection model

Table 1 illustrates that the Whale Optimization Algorithm (WOA) inside the proposed Adaptive Whale-Optimized Neural Intelligence framework emulates the hunting behavior of humpback whales to optimally adjust neural network parameters for cyber-attack detection. A population of whales is randomly produced, with each whale symbolizing a proposed solution, including neural weights and biases. Following preprocessing and adaptive feature extraction from the CIC-IIoT-2025 dataset, a fitness function generally grounded on detection accuracy and error minimization is assessed for each whale. The program repeatedly adjusts whale locations by three fundamental mechanisms surrounding the optimal solution to utilize advantageous areas, spiral movement to enhance solutions near the optimum, and random search to investigate fresh regions and prevent premature convergence. In each cycle, the most effective whale is chosen to direct the population's movement. This adaptive optimization persists until convergence, yielding an improved neural model that attains excellent accuracy and resilience in detecting cyber-attacks in Industrial IoT.

3.5 Artificial Neural Network

The proposed Artificial Neural Network (ANN) serves as the central leaming and decision-making module. Following data preprocessing

and adaptive feature extraction, the chosen features are input into a multi-layer neural network engineered to adjust its architecture and parameters in response to changing IIoT traffic patterns. ANN is attained by the continual modification of network weights, learning rate, and hidden neuron activation in response to input from classification performance. The Whale Optimization Algorithm (WOA) facilitates this adaptation by improving neural parameters to reduce classification error and enhance attack detection accuracy. This integration allows the neural model to effectively leam both normal and harmful traffic patterns, manage non-linearity and highly dimensional information, and enhance generalization in either to unencountered cyber-attack situations. The adaptive neural network delivers resilient, scalable, and high-accuracy intrusion detection in Industrial loT settings

Table 2: ANN Pseudocode

Input: Preprocessed and extracted feature set X. Labels Y
Output: Trained Adaptive Neural Network Model
Step 1. Initialize neural network architecture (input, hidden, output layers)
Step 2. Randomly initialize weights and biases
Step 3. Define fitness function (maximize accuracy /minimize loss)
Step 4. While stopping criteria are not met:
a. Forward propagate input X through the network
b. Compute output predictions $\hat{Y}$
c. Calculate loss using Y and $\hat{Y}$
d. Update neural weights and biases using WOA-optimized parameters
e. Adapt learning rate and neuron activations
Step 5. Select the best optimized neural configuration
Step 6. Output the final trained model for attack detection

Table 2 displays the pseudocode that delineates an ANN training procedure enhanced by the whale optimization algorithm for attack detection. The network design is first established with input, hidden, and output layers, and the weights and biases are assigned randomly. A fitness function is formulated to direct optimization by maximizing accuracy or decreasing loss. During training, input features are propagated forward through the network to produce predictions, and the loss is calculated in relation to the true labels. The WOA algorithm is used to adjust weights and biases, while learning rates and neuron activations are constantly modified to enhance performance. The process continues until the stopping requirements are satisfied, at which point the most efficient neural configuration is chosen and presented as the final trained model for attack detection.

3.6 Adaptive Whale Optimized Neural Intelligence (AWONT) Classification

The AWONI model for detecting cyberattacks in Industrial IoT contexts combines the optimization features of the WOA with an adaptive neural network to improve classification efficacy. Table 3 pseudocode illustrates that the process starts with preprocessed IoT data, from which pertinent characteristics are extracted to create the input dataset. The neural network design has input, hidden, and output layers, with weights and biases given randomly after initialization. The model then establishes a fitness function designed to optimize classification accuracy while reducing prediction loss. During training, input characteristics are transmitted through the network to produce output predictions, which are then compared to true labels to compute loss. The WOA optimizes neuronal weights and biases by mimicking the encircling and hunting behaviors of whales, enabling the network to adaptively modify learning rates and neuron activations for enhanced learning efficiency. Iterations persist until convergence or predefined stopping conditions are met, guaranteeing the identification of the optimal network design. The end product is a sophisticated, trained AWONI model proficient in reliably identifying cyber assaults inside intricate Industrial IoT settings, integrating adaptive learning with evolutionary optimization for enhanced categorization.

Table 3: AWONI Classification

Input: Preprocessed IoT feature set X, Labels Y
Output: Trained AWONI model for attack detection
Step 1: Initialize Neural Network Architecture
- Define the number of neurons in the input, hidden, and output layers.

Step 2: Randomly Initialize Weights and Biases
- W ← random weights
- b ← random biases

Step 3: Define Fitness Function
- Fitness maximize accuracy/minimize loss

Step 4: Initialize Whale Optimization Algorithm (WOA) Parameters
- Population of whales P
- Maximum iterations T
- Position vectors correspond to neural network weights

Step 5: While stopping criteria not met (iteration <T):

a. Forward Propagation
- Compute network output predictions Ý from input X

b. Compute Loss
- Loss= LossFunction(Y, Y)

c. WOA based Optimization
- Update positions of whales (weights & biases) using encircling, bubble-net, and search behaviors

d. Adapt Learning Parameters
- Adjust learning rate and neuron activations based on fitness feedback

Step 6: Select Best Whale Position
e. BestWeights, Best Biases corresponding to the highest fitness
Step 7: Update Neural Network
f. Set network weights and biases to Best Weights, BestBiases
Step 8: Output
g. Trained AWONI model ready for cyberattack detection

Table 3 presents the AWONI model for cyber threat detection in industrial loT settings, integrating an adaptive neural network with the Whale Optimization Algorithm (WOA). The network design is established with input, hidden, and output layers, and the weights and biases are initialized randomly. A fitness function is established to optimize classification accuracy and minimize loss. During training, input features are propagated forward through the network to provide predictions, and the loss is calculated. WOA subsequently enhances the network by modifying weights and biases via encircling, bubble-net, and search behaviors, while learning rates and neuron activations are adaptively calibrated according to performance. The iterative procedure continues until die stopping requirements are satisfied, at which point the optimal configuration is chosen. The end product is a trained AWONI model proficient in reliably identifying cyber assaults inside complex Industrial loT systems.

3.7 Attack Classification

It is the responsibility of this module to classify traffic as normal, abnormal, or particular attack kinds. Multi-class classification is carried out by the system via the use of the learned adaptive neural model. This enables the system to conduct fine-grained detection and situational awareness in industrial networks.

3.8 Alert Generation and Threat Analysis

Real-time notifications are triggered whenever an attack is detected, which enables speedy mitigation. Through the study of attack intensity, frequency, and impacted assets, the threat analysis module contributes to the improvement of the resilience of the IIoT system. This module also helps with forensic investigation and reaction preparation.

3.9 Performance Metrics

The performance metrics used to evaluate the Adaptive Whale-Optimized Neural Intelligence (AWONT) model for cyberattack detection in Industrial IoT environments.

A. Accuracy:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Accuracy measures the overall correctness of the model by calculating the ratio of correctly predicted instances (both attacks and normal traffic) to the total instances. Here

TP: True Positives (correctly detected attacks), TN: True Negatives (correctly detected normal

traffic), FP: False Positives (normal traffic incorrectly classified as attacks), FN: False Negatives (attacks missed by the model). Accuracy gives a general sense of performance but can be misleading if the dataset is imbalanced.

B. **Precision:**

$$Precision = \frac{TP}{TP + FP}$$

Precision measures the proportion of correctly detected attacks out of all instances classified as attacks by the model. High precision indicates the model makes fewer false alarms, which is critical in industrial IoT environments to avoid unnecessary responses to false threats.

C. Recall

$$Recall = \frac{TP}{TP + FN}$$

Recall quantifies the model's ability to correctly identify actual attacks. High recall ensures that most real cyberattacks are detected, minimizing the risk of security breaches in Industrial loT systems.

D. F1-Score

$$F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall}$$

The Fl-score provides a harmonic mean of precision and recall, balancing the trade-off between false positives and false negatives. It is especially useful when dealing with imbalanced datasets, common in cyberattack detection, ensuring the model performs well in both detecting attacks and avoiding false alarms.

4. Results and Discussions.

The AWONI model for cyber threat detection in Industrial loT scenarios underscores both the model's efficacy and its computational demands. The AWONI model was executed in Jupyter Notebook, which provides an interactive environment conducive to experimenting with machine learning methods, displaying outcomes, and rapidly debugging code. The tests were performed on a machine equipped with an Intel i5 CPU, 12 GB of RAM, and Windows 11 as the operating system, offering enough computing capabilities for training the adaptive neural network optimized using the WOA. A variety of Python packages were employed to aid in the implementation and assessment of the model, including NumPy and Pandas for data preprocessing and feature manipulation, TensorFlow/Keras or PyTorch for neural network construction and training. Scikit-learn

for performance metrics and data partitioning, and Matplotlib/Seaborn for result visualization. Notwithstanding the iterative characteristics of WOA optimization and the computational requirements of neural network training, the system adeptly managed forward propagation, loss computation, and weight adjustments without notable delay, indicating that AWONI can be effectively implemented on mid-range hardware. The findings indicate that the model attained elevated accuracy, precision, recall and FI-score, confirming the efficacy of AWONI for cyberattack detection in Industrial IoT systems, while emphasizing that practical use does not need advanced computing resources.

Figure 2: Sample Dataset

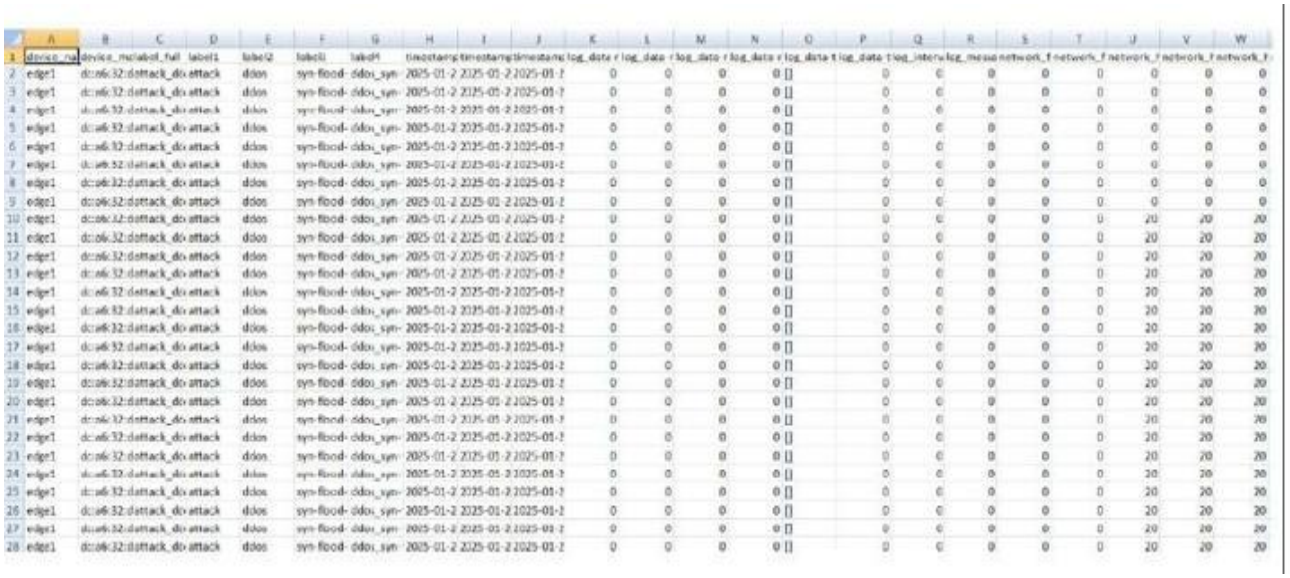

Figure 2 displays that the original CIC-IIoT dataset comprises 90,391 records with 94 attributes, including a varied array of network traffic characteristics and threat classifications. During preprocessing, duplicate entries were detected and rectified to enhance data consistency and model generalization, yielding a refined dataset of 136,800 instances with 94 characteristics post-consolidation. Missing values were methodically addressed to avoid biased learning and training instability. Categorical characteristics, including protocol kinds and attack labels, were converted into numerical representations by Label Encoding, facilitating interoperability with machine learning and deep learning techniques. Feature scaling was then included to equalize the data distribution, guaranteeing equal contribution of all features during model training and enhancing convergence speed. Following the separation of the target label, the dataset was divided into training and testing subsets via a stratified method. The resulting preprocessed dataset

comprises 67,793 training samples and 22,598 testing samples, each including 93 input attributes, hence assuring balanced class representation and dependable performance assessment. The sanitized and modified dataset was subsequently stored successfully for effective reutilization in classification trials. The preprocessed summary Table 4 is displayed.

Table 4: Preprocessing Summary

Dataset Description	Values
Original Data Set	(60525, 94)
Filtered Data Set	(30842, 93)
Training Set	(23131,93)
Testing Set	(7711,93)
Encoded Label Range	0 to 82
Total Classes	83

Features like label_full and timestamp have very high variance, meaning they differ widely across instances. Such features are informative for classification because they capture diverse attack types and timing patterns. Labell has zero variance, meaning it is constant for all samples. These features may not contribute meaningfully to the model and can sometimes be dropped to reduce complexity. Features like device_name and device_mac are encoded numerically. Their mean and variance show the spread of different devices in the dataset, which is crucial for tracking attack sources. Timestamp, timestamp_start, and timestamp_end capture the temporal behavior of traffic and attacks. Including these allows models like AWONI to leverage time-dependent patterns in cyberattack detection

Features	Mean	Variance
device_name	17.243090	1608180e+02
device_mac	17.620867	1.505076e+02
label_full	445.001338	6.860337e+02
label1	0.000000	0.000000e+00
Label2	2.41145	2.332309e+00
Label3	29.827972	2.935118e+02
Label4	42.815349	6.060433e+02
timestamp	30002.125138	3.033035e+08
timestamp_start	26259.919471	2.224675e+08
timestamp_end	26261.324048	2.224815e+08

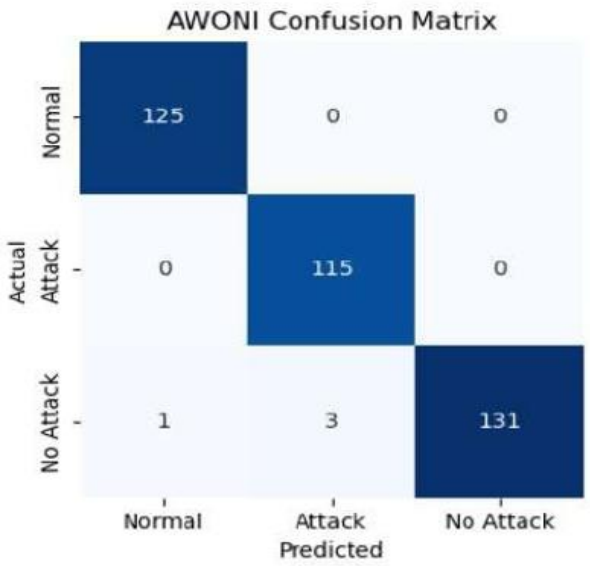

Figure 3: Confusion Matrix

Figure 3 displays the classification performance of the proposed model across three classes: Normal, Attack, and No Attack. The model properly classifies 125 Normal cases, 115 Attack instances, and 131 No-Attack instances, which are depicted along the major diagonal of the matrix and demonstrate a good true-positive performance for all classes. Very few misclassifications are observed: just one No-Attack case is improperly predicted as Normal, and three No-Attack examples are misclassified as Attack, while no Normal or Attack samples are inappropriately classified into other categories. This little misunderstanding illustrates that the AWONI model successfully differentiate between benign traffic and malicious activity, enabling excellent accuracy and resilience in multi-class cyber-attack detection for Industrial IoT contexts.

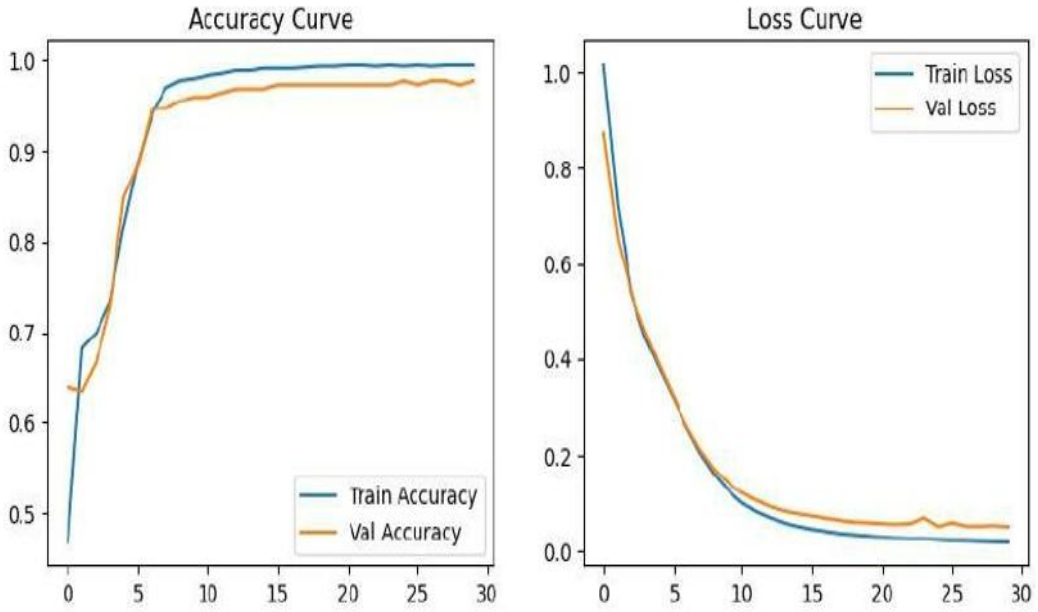

Figure 4: Accuracy and Loss

Figure 4 demonstrates the effective learning and convergence behavior of the AWONI model during training. In the accuracy plot, both

training and validation accuracy increase rapidly in the initial epochs, indicating that the model quickly captures the underlying patterns in the data. After approximately 8-10 epochs, the curves stabilize near a high accuracy level, with only a small gap between training and validation accuracy, which suggests good generalization and minimal overfitting. Similarly, the loss curve shows a sharp decrease in both training and validation loss during the early stages, followed by a gradual flattening as the model converges. The close alignment between training and validation loss further confirms the stability of the learning process. Overall, these trends indicate that the AWONI model achieves fast convergence, robust performance, and reliable classification capability for attack detection in Industrial IoT environments.

5. Conclusion

An Adaptive Whale-Optimized Neural Intelligence (AWONI) framework for efficient cyberattack detection in Industrial Internet of Things (IoT) scenarios was provided in this paper. The suggested model effectively represents the intricate and nonlinear attack patterns found in IIoT traffic by combining adaptive neural leaming with Whale Optimization-based parameter adjustment. While retaining excellent detection accuracy, the model's resilience against a variety of attack behaviors is improved by the integration of dynamic feature extraction and adaptive learning techniques. Experimental results demonstrate that AWONI achieves superior classification performance across Normal, Attack, and No-Attack classes, with strong generalization capability and minimal misclassification. The stable convergence observed in accuracy and loss curves further validates the reliability of the approach. Overall, the AWONI framework offers a scalable, intelligent, and computationally efficient solution for real-time cyberattack detection, making it well-suited for deployment in resource-constrained and security-critical Industrial IoT systems.

References

1) Berrios, S., Leiva, D., Olivares. B. Allende-Cid, H., & Hermosilla, P. (2025). Systematic Review: Malware Cybersecurity. Applied Sciences, 15(14), Detection and Classification https://doi.org/10.3390/app15147747 in 7747.

2) Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyberattacks and cybersecurity vulnerabilities in the university sector. Computers, 14(2), 49. https://doi.org/10.3390/computers 14020049

3) Awajan, A. (2023). A novel Deep Learning-Based intrusion detection system for loT nerworks. Computers. 12(2), 34. https://doi.org/10.3390/computers 12020034

4) Al-Shuareeda, M. A.. Manickan, S., & Saare,

M. A (2022). DDoS attacks detection using machine learning and deep learning techniques analysis and comparison. Bulletin of Electrical Engineering and Informatics, 12(2), 930-939. https://doi.org/10.11591/eci. v1212.4466

5) Zhang, J., Pan, L., Han, Q., Chen, C., Wen, S., & Xiang, Y. (2021). Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. IEEE CAA Journal of Automatica Sinica, 9(3), 377-391. https://doi.org/10.1109/jas 2021.1004261

6) Villafianca, A., Thant, K. M., Tasic, L., & Cano, M. (2025). Al-Enabled IoT Intrusion Detection: Unified Conceptual Framework and Research Roadmap. Machine Learning and Knowledge Extraction, 7(4), 115. https://doi.org/10.3390/make7040115

7) Ahmad. Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2020), Network intrusion detection system: A systematic study of machine learning and deep learning upproaches. Trameactions on Emerging Telecommunications Technologies, 32(1). https://doi.org/10.1002/ett.4150

8) Qiqieh, L. Alzubi, O., Alzubi, J., Sreedhar, K. & Al-Zoubi, A. M.. (2024). An intelligent cyber threat detection: A swarm-optimized machine learning approach, Alexandria Engineering Journal, 115, 553-563. https://doi.org/10.1016/j.j.2024.12.039

9) Feng, H.. Cao, K., Huang, G., & Lin, H. (2024) ABWOA: adaptive boundary whale optimization algorithm for large-scale digital twin network construction. Journal of Cloud Computing Advances Systems and Applications, 13(1). https://doi.org/10.1186/s13677-024-00667-z

10) Chen, Y. (2025). Efficient task allocation in the Internet of Things using Levy Flight-Driven Walrus optimization. International Journal of Advanced Computer Science and Applications, 16(5). https://doi.org/10.14569/ijacsa.2025.0160555

11) Shan, L. (2025), (IoT) Network intrusion detection system using optimization algorithms. Scientific Reports, 15(1), 21706. https://doi.org/10.1038/s41598-025-04638-5

12) Alsaidi, S. A. A A.. Ogaili. R. R. N. A.. Alyasseri, Z. a. A. Al-Shamunary, D., Ibaida, A. & Słowik, A. (2025). Multi-objective Markov-enhanced adaptive whale optimization cybersecurity model for binary and multi-class malware cyberthreat classification. Journal of Electronic Science and Technology, 23(4), 100334. https://doi.org/10.1016/j.jnlest.2025.100334

13) Li, L., Siakam, D., Liu, J., & Zheng, Y. (2025), IWOA-BP neural network for cybersecurity assessment in industrial IoT-enabled smart manufacturing systems. Advances in Mechanical Engineering, 17(10). https://doi.org/10.1177/16878132251388267

14) Gotarane, V., Abimannan, S., Hussain, S., & Irshad, R. R. (2024). A hybrid framework leveraging whale optimization and deep

learning with Trust-Index for attack identification in IoT networks. IEEE Access, 12. 36296-36310. https://doi.org/10.1109/necess 2024.3374691

15) Masaud, M. a. A., Aver, S. A., & Rahebi, J. (2025). Detecting cyberattacks in smart grids using VGG-16 and whale-fisher mantis optimization algorithm (WOA-FMO). The Journal of Supercomputing. 81(7). https://doi.org/10.1007/s11227-025-07345-0

16) Jyethi, K. K., Borna, 5. R., Stilakslani, K., Balachandran, P. K., Redly, G. P., Colak, 1., Dhananjayulu, C., Chinthaginjala, R., & Khum, B. (2024) A novel optimized neural network model for cyber attack detection using an enhanced whale optimization algorithm. Scientific Reports, 14(1), 5590. https://doi.org/10.1038/s41598-024-55098-2

17) Albayan, F., Alruwais, N., Alamgeer, M., Alashjace, A. M. Abdullah, M., Khadidos, A. O., Alallalı, F. S., & Alshareef, A. (2025). Design of advanced intrusion detection in cybersecurity using an ensemble of deep learning models with an improved beluga whale optimization algorithm. Alexandria Engineering Journal, 121,90 102. https://doi.org/10.1016/j.acj.2025.02.069

18) Cum, J., Shu, L., & Alkhayyat, A. (2025). Enhanced security for tol cloud environments using Efficient Net and an enluneed football team training algorithm. Scientific Reports, 15(1), 20764. https://doi.org/10.1038/s41598-025-08343-1

19) Behera, A., Sahoo, K. S., Mishra, T. K., & Bhuyan, M. (2024) A combination learning framework to attacks in IoT networks. Internet of Things, 28. 101395, uncover cyber https://doi.org/10.1016/j.jot.2024.101395

20) Hwaitat, A. K. A., & Fakhouri, H. N. (2024). Adaptive Cybersecurity Neural Networks: An evolutionary approach for enhanced attack detection and classification. Applied Sciences, 14(19) 9142. https://doi.org/10.3390/app14199142

21) Srikanth, M., Sunitha, P., Puppala, R. S., Kumar, A. S., & Akshaykranth. A. (2025). A Novel Framework for Intrusion Detection in IOT Networks using Hybrid Optimization Algorithm and Convolutional Neural Networks. Franklin Open, 100461. https://doi.org/10.1016/j. fraope. 2025.100461

22) Elsedimy, E L., & AboHashish, S. M. M. (2025). An intelligent hybrid approach combining fuzzy C-means and the spem whale algorithm for cyber attack detection im IoT networks. Scientific Reports, 15(1), 1005. https://doi.org/10.1038/s41598-024-79230-4

23) Jothi, K. R. & Vaithiyanathan, B. (2024). Developing a Hybrid Approach with Whale Optimization and Deep Convolutional Neural Networks for Enhancing Security in Smart Home Environments Sustainability Through IoT Devices. Sustainability, 16(24), 11040. https://doi.org/10.3390/sa162411040

24) Rahman, A., Hossain, M. S., Muhammad,

G., Kundu, D. Debnath, T., Rahman, M., Khan, M. S. I.. Tiwari, P. & Hand. S. S. (2022). Federated learning-based Al approaches in smart healthcare: concepts, laxonomies, challenges, and open issues. Cluster Computing. 26(4), 2271-2311. https://doi.org/10.1007/s10586-022-03658-4

25) Aluri, Y. K., Devi, V. S. A., Chinthakunta, M., Manmur, M., Jayapal, P. K., Baian, G., & Leila, K. K. (2024). Detection of Forest Fire Using Modified LSTM-Based Feature Extraction with Waterwheel Plant Optimisation Algorithm-Based VAE-GAN Model. International Journal of Safety and Security Engineering, 14(2), 329-340. https://doi.org/10.18280/tisse. 140202

26) Alblehai, F. (2025). Artificial intelligence-driven cybersecurity system for intermet of Things using self-attention deep learning and metaheuristic algorithms Scientific Reports, 15(1), 13215. https://doi.org/10.1038/41598-025-98056-2

27) Alamro, H., Mansouri, W., Saeedi, K., Alshammeri, M., Aljabri, J., Alotaibi, F. A., Negm, N., & Sharif, M. M. (2024) Modeling of Bayesian-Based Optimized transfer learning model for Cyber-Attack detection in Internet of Things assisted resource constramed systems. IEEE Access, 12, 177298-177311. https://doi.org/10.1109/access.2024.3482876

28) Binbusayyis, A., & Vaiyapuri, T. (2021). Unsupervised deep learning approach for network intrusion detection combining a convolutional autoencoder and a one-class SVM. Applied Intelligence, 51(10), 7094-7108. https://doi.org/10.1007/s10489-021-02205-9

29) Kiruthikkunar, A. Maheswari, N. U., Poukuunar, D. D. N., Alhaned, A. N., Salma, S. N., & Saravanakumar, R. (2025). Enhancing the Efficacy of Machine Learning-Based Intrusion Detection Systems on an Imbalanced and Contemporary Dataset. 2025 International Conference on Advanced Computing Technologies. (ICOACT), 1-6. https://doi.org/10.1109/iccact63339.2025.11004649

30) Jeevanantham, M., Shanmugalakshmi, N., Sudhakar, S., Babu, M. C., Ramanan, K., & Saravanakumar, R. (2025). Madhine Learning Techniques for Intrusion Detection System Malware on Android Devices. 2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI), 15. https://doi.org/10.1109/icdsaai65575.2025 11011568

31) Sivarajan, S., & Jebaseelan, S. S. (2022). An efficient adaptive deep neural network model for securing demand side management in IoT-enabled smart grid. Renewable Energy Focus, 42, 277-284. https://doi.org/10.1016/j.ref.2022.08.003

32) Alotaibi, S. S., & Alghamdi, T. A. (2025). Deep learning with league championship algorithm-based intrusion detection on cybersecurity-driven industrial IoT systems. Scientific Reports, 15(1), 30296.

https://doi.org/10.1038/s41598-025-15464-0

33) Rawajbeh, M. A., Soosni, A. J. M., Ramasanmy, L. K., & Khan, F. (2025). Trustworthy Adaptive Al for Real-Time Intrusion Detection in Industrial IoT Security. IoT, 6(3), 53. https://doi.org/10.3390/iot6030053

34) Bee, J. Y., Vanithamani, S., Shanmugapriya, S., Devi, K. N., Nallasivan, G., Ponkumar, D. D. N. & Saravanakumar, R. (2025). Application of Machine Leaming to Optical Network Traffic-Driven Provisioning Services. 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI), 1073-1077, https://doi.org/10.1109/iccsai64074.2025.1106-4579

35) P. H. P. A A., Lakshmi, A. A., Ragavendran, N. Purushothaman, K. E. Maheswari, G. U., & Saravanakumar, R. (2024). Advancements in Cybersecurity Using Deep Leaming Techniques: Attack Detection for Trojan Horses. 2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT), 1-6 https://doi.org/10.1109/iceect51 758 2024.10739164.