# Toward Intelligent Cyber Defense: An Optimized CNN–LSTM Framework Powered by Particle Swarm Optimization


1st Nongmeikapam Thoiba Singh
*Department of CSE*
*UIE, Chandigarh University*
Mohali-140413, Punjab, India
nthoiba12@gmail.com

2nd Ankit Gupta
*Department of CSE*
*UIE, Chandigarh University*
Mohali-140413, Punjab, India
ankitgupta93688@gmail.com

3rd Prakash Kumar
*Department of CSE*
*UIE, Chandigarh University*
Mohali-140413, Punjab, India
prakashjha134590@gmail.com

4th Shivam Kumar
*Department of CSE*
*UIE, Chandigarh University*
Mohali-140413, Punjab, India
shivam40180@gmail.com

5th Aryan Kumar
*Department of CSE*
*UIE, Chandigarh University*
Mohali-140413, Punjab, India
Kashyap10032005@gmail.com

6th Aryan Kumar
*Department of CSE*
*UIE, Chandigarh University*
Mohali-140413, Punjab, India
aryankumar3206@gmail.com



***Abstract*—The rising complexity of cyberattacks, including DDoS attacks, ransomware, and advanced persistent threats, requires the development of intelligent and adaptive intrusion detection systems. In this context, this paper proposes an optimized hybrid deep learning approach based on Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks and Particle Swarm Optimization (PSO) for effective cyberattacks detection. The proposed approach is optimized using PSO for the critical parameters of the proposed model, including the learning rate, the number of convolutional filters, and the number of LSTM units. The proposed approach is implemented and tested using the intrusion detection datasets, and the results are compared using various performance metrics. The results of the proposed approach show that the optimized CNN-LSTM model has an accuracy of 99.12%, precision of 98.94%, recall of 99.08%, and F1-score of 99.01%, with a false positive rate of 0.87% and AUC of 0.998. Additionally, the proposed approach has better computational efficiency with reduced training time and average inference time of 0.0043 seconds per sample. The results of the proposed approach are significant in the development of effective intrusion detection systems using the optimized hybrid deep learning approach and PSO for effective cyberattacks detection.**



***Index Terms*—Cyber Threat Detection, CNN–LSTM, Particle Swarm Optimization, Deep Learning, Intrusion Detection System, Network Security, Swarm Intelligence, Hyperparameter Optimization, Malware Detection, Intelligent Cyber Defense.**


## I. Introduction

The high digitization of the contemporary infrastructures such as cloud computing, IoT ecosystems, smart cities, and the Industry 4.0 platform has amplified greatly the attack surface. Modern incidents of cyber-attacks like Distributed Denial of Service (DDoS), ransomware, phishing, botnets and Advanced Persistent Threats (APTs) are increasingly becoming dynamic and sophisticated and are becoming sneaky [1], [2]. Conventional rule based and signature based intrusion detection systems (IDS) have difficulties relating to the detection of zero-day exploits and polymorphic malware as they rely on predefined attack signatures [3], [4]. This has necessitated the establishment of intelligent, adaptive and data-driven cybersecurity systems to safeguard contemporary network infrastructures [5]. The application of machine learning (ML) as an intrusion detection method has become very popular because it can be trained using past information and apply the lessons to novel attacks [6], [7]. Classical ML algorithms like Support Vector machines (SVM), random forests (RF) and k-Nearest Neighbors (k-NN) have proven themselves to be promising in the tasks of anomaly and misuse detection [8], [9]. Though, such models are frequently based on manual feature engineering and can be hard to learn about subtle spatial-temporal forces that exist in large scale network traffic data [10]. The increasing quantity, speed, and nature of cybersecurity data require more representation learning methods with more powerful features of automated features extraction [11]. Deep learning (DL) models have become a strong competitor because of their hierarchical learning features of features [12]. Convolutional Neural Networks (CNNs) are especially useful in the extraction of the spatial features and recognising the hidden attack signatures in network flow matrices and packet payload representations [13], [14]. In the meantime, Recurrent Neural Networks (RNNs), particularly, Long Short-Term Memory (LSTM) networks, are created to take into consideration temporal and sequential associations in

time-series information, which is why they are appropriate to describe time-varying attacks and multiphase attack patterns [15], [16]. Nevertheless, either CNN or LSTM model can potentially not utilize both spatial and temporal features at the same time. To overcome this shortcoming, it has been suggested that hybrid CNNLSTM networks be used to harness the capabilities of the spatial feature extraction alongside the temporal sequence modeling [17], [18]. These integrated models have demonstrated better detection of complicated and elusive cyber threats as opposed to standard ML methods. However, the success of deep hybrid models strongly relies on the optimal choice of the hyperparameters, such as the learning rate, the number of convolutional filters, the sizes of the kernel, the number of hidden units, the dropout rates, and the batch size [19]. The methods of manual tuning or grid search are process-intensive and do not necessarily yield global optimum. Metaheuristic optimization algorithms have been of much interest in hyperparameter tuning of deep learning systems [20]. Particle Swarm Optimization (PSO), which is based on the social behavior of bird flocking and fish schooling, is one of them and has been demonstrated to be effective in searching large spaces and converging to optimum solutions with less computing overhead [21]. PSO improves the generalization ability of models by automatically choosing the best combinations of parameters, which decreases the overfitting and increases the detection accuracy. In our paper, we will suggest an optimized CNNLSTM structure to be used in conjunction with Particle Swarm Optimization to detect intelligent cyber threats. The CNN component is used to generate the high-level spatial representations of the network traffic data and the LSTM module is used to extract the temporal dependencies as well as patterns of attack evolution. PSO is used to optimize important hyperparameters in order to have better classification. The model that is proposed will improve the quality of detection, reduce the number of false positives, and increase the efficiency of the computation to aid in the creation of a strong, adaptive, and scalable cybersecurity defense mechanism.

## II. Literature Review

Significant research developments in the field of cybersecurity have shown the increasing trends and integration of deep learning, optimization algorithms, and hybrid models to enhance cyber threat detection in IoT and futuristic network systems. Nandagopal et al. proposed a deep learning-based cyber threat detection framework with integration into blockchain technology to preserve privacy in 6G IoT systems [1]. The authors have shown improved detection capability and efficient management of cyber threats with the proposed framework. Markkandeyan et al. have introduced a hybrid deep learning-based model integrated with optimization algorithms to enhance the detection and identification of cyber threats in futuristic network systems [2]. Benmalek and Seddiki have integrated particle swarm optimization with machine learning and deep learning models to enhance feature selection and intrusion detection in IoT systems [3]. Additionally, Birthriya et al. have proposed a CNN–SVM-based phishing website detection framework with integration into nature-inspired algorithms to enhance the accuracy of the proposed framework [4]. Alzeyadi et al. have proposed an efficient and lightweight spam detection model with integration into Rüppell's fox optimizer for social media platforms [5]. Table I shows the Comparative Analysis of Recent Cybersecurity Threat Detection Models.

Rawat et al. (2025) studied the propagation of vulnerability in online social networks and its impact on cybersecurity risk assessment [6]. Moreover, Turaka and Panigrahy (2025) proposed an efficient quantum-driven chaos-informed deep learning framework for intrusion detection and feature selection in IoT networks [7], while Swetha et al. (2025) proposed an efficient hybrid metaheuristic-driven intrusion detection system with swarm-based optimization [8]. Additionally, Al-E'mari et al. (2025) proposed an efficient quantum epigenetic algorithm-based adaptive cybersecurity threat detection system [9]. Several researchers have also proposed various intrusion detection models and efficient optimization algorithms for enhancing the security level in IoT networks. Bahulayan and P (2025) proposed an efficient firefly-based optimization algorithm to enhance the security level in 5G IoT cyber-physical systems [10], while Bensaoud and Kalita (2025) proposed efficient hybrid deep learning models that improved the performance level in cyber-attack detection in IoT networks [11]. The overall AI-based cybersecurity scenario was discussed by Syllaidopoulos et al. (2025) with respect to various applications and challenges faced by AI in the cybersecurity and counter-terrorism domains [12]. Lmkaiti et al. (2025) proposed an efficient metaheuristic algorithm-based RPL protocol security in IoT networks under attack scenarios [13].On the other hand, Nandhini et al. proposed a deep learning architecture with a hidden layer to detect cyber attacks in IoT-WSN systems [14]. Furthermore, Kumar and Neduncheliyan proposed an ensemble deep learning architecture inspired by sharks to improve the security of smart city IoT systems [15]. Additionally, Elberri et al. proposed an ensemble-based phishing detection model utilizing an African Vulture Optimization and game theory-based LSTM-CNN [16], while Sheikhi and Kostakos improved the detection efficiency of malicious websites utilizing an ensemble-based XGBoost and PSO algorithm with firefly-based feature selection [17]. Moreover, Ahmad et al. proposed an ensemble-based optimized detection model utilizing an optimization technique to detect malware attacks in IoT systems [18], while Ahmed et al. proposed an ensemble-based optimized detection model with advanced feature selection to detect network intrusion attacks [19]. Furthermore, Alabdulatif et al. proposed an ensemble-based detection model utilizing machine learning to detect IoT-based DoS and DDoS attacks [20], while Patil and Joshi proposed an arachnid swarm-based CNN to significantly enhance the efficiency of intrusion detection systems [21].

## III. Methodology

The suggested methodology is divided into four key steps such as data preprocessing, the construction of the hybrid

TABLE I
COMPARATIVE ANALYSIS OF RECENT CYBERSECURITY THREAT DETECTION MODELS

| Ref No. | Title | Authors & Year | Key Findings | Research Gaps |
|---|---|---|---|---|
| [1] | Cyber threat detection in 6G IoT using DL and blockchain | C. Nandagopal et al., 2026 | Integrated deep learning with blockchain for privacy-preserving 6G-IoT threat detection; improved security and data integrity. | High computational overhead; scalability issues in real-time 6G environments not fully validated. |
| [2] | Hybrid deep learning cyber security threat detection model | S. Markkandeyan et al., 2025 | Hybrid DL model with optimization improved detection accuracy and convergence speed. | Limited evaluation on heterogeneous IoT datasets; lack of explainability analysis. |
| [3] | PSO-enhanced ML/DL for IoT intrusion detection | M. Benmalek and A. Seddiki, 2025 | PSO improved feature selection and classification accuracy for IDS systems. | Performance under zero-day attacks not explored; real-time deployment constraints missing. |
| [4] | CNN-SVM phishing detection with hyperparameter tuning | S. K. Birthriya et al., 2025 | Nature-inspired tuning enhanced phishing detection precision and recall. | Generalization across multilingual phishing datasets not analyzed. |
| [5] | Explainable spam detection with Rüppell's fox optimizer | H. Alzeyadi et al., 2025 | Lightweight and explainable spam classifier suitable for social media platform X. | Cross-platform adaptability and adversarial robustness not evaluated. |

CNN-LSTM model, hyperparameters optimization using Particle Swarm Optimization (PSO), and the assessment of performance. Benchmark intrusion detection datasets are first gathered and pre-processed to eliminate noise, missing data and redundant attributes. Label encoding or one-hot encoding is used to encode categorical features like protocol type, service, and flag. Min–Max normalization is used to do feature scaling to normalize the values to facilitate even distribution of values, and to hasten the convergence of the model. An 80:20 split is chosen to divide the dataset into training and testing subsets hence rendering unbiased performance appraisal. Fig. 1 shows the proposed methodology used in this research paper.

### A. Convolution Operation

The spatial feature extraction using CNN is defined in (1).

$$F_i^{(l)} = \sigma\left(\sum_{j=1}^{M} W_{ij}^{(l)} * X_j^{(l-1)} + b_i^{(l)}\right) \tag{1}$$

where $F_i^{(l)}$ represents the $i^{th}$ feature map at layer $l$, $W_{ij}^{(l)}$ denotes the convolution kernel weights, $X_j^{(l-1)}$ is the input from the previous layer, $b_i^{(l)}$ is the bias term, $*$ denotes convolution operation, and $\sigma(.)$ is the activation function (e.g., ReLU).

This equation enables automated spatial feature extraction from network traffic data.

### B. LSTM Memory Update

The temporal dependency modeling in LSTM is expressed in (2).

$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t \tag{2}$$

where $C_t$ is the current cell state, $C_{t-1}$ is the previous cell state, $f_t$ is the forget gate, $i_t$ is the input gate, $\tilde{C}_t$

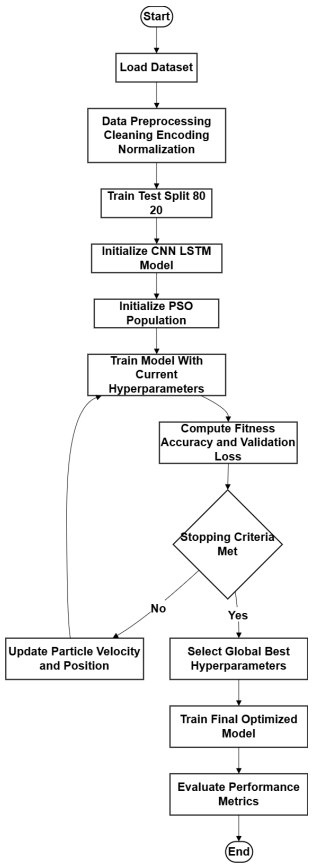


Fig. 1. Proposed Methodology

is the candidate cell state, and $\odot$ represents element-wise multiplication.

This formulation allows retention of long-term sequential attack patterns.

### C. PSO Velocity Update

The velocity update rule in Particle Swarm Optimization is defined in (3).

$$v_i^{t+1} = wv_i^t + c_1 r_1 (pbest_i - x_i^t) + c_2 r_2 (gbest - x_i^t) \quad (3)$$

where $v_i^t$ is the velocity of particle $i$ at iteration $t$, $w$ is the inertia weight, $c_1$ and $c_2$ are cognitive and social coefficients, $r_1$ and $r_2$ are random numbers in $[0, 1]$, $pbest_i$ is the personal best position, $gbest$ is the global best position, and $x_i^t$ is the current position.

This equation balances exploration and exploitation during hyperparameter optimization.

### D. Objective (Fitness) Function

The optimization objective for classification is defined in (4).

$$\mathcal{F} = \alpha(1 - Accuracy) + \beta(Loss) \quad (4)$$

where $\mathcal{F}$ is the fitness value, $Accuracy$ represents classification accuracy, $Loss$ denotes validation loss, and $\alpha$, $\beta$ are weighting factors.

Minimizing this objective ensures improved detection performance and reduced overfitting.

**Algorithm 1** PSO-Optimized CNN–LSTM for Cyber Threat Detection

```
Initialize particle swarm with random hyperparameters
Initialize velocities v_i and positions x_i
Define fitness function using Eq. (??)
for each iteration t = 1 to MaxIter do
    for each particle i do
        Configure CNN–LSTM using x_i
        Train model on training dataset
        Compute fitness F_i
        if F_i < pbest_i then
            Update personal best pbest_i
        end if
    end for
    Update global best gbest
    for each particle i do
        Update velocity using Eq. (??)
        Update position: x_i^{t+1} = x_i^t + v_i^{t+1}
    end for
end for
Train final CNN–LSTM using optimal gbest
Evaluate model using Accuracy, Precision, Recall, F1-score
return Optimized Cyber Threat Detection Model
```

Algorithm 1 depicts the PSO, Optimized CNN, LSTM for Cyber Threat Detection. At the core, the framework architecture is a hybrid of Convolutional Neural Networks (CNN) and Long Short, Term Memory (LSTM) networks. The CNN part is designed to automatically extract structured network traffic data spatial features by means of multiple convolutional layers, activation and pooling operations. These layers reveal hidden attack signatures, along with the development of higher, level traffic pattern abstractions. The obtained feature maps are then reformed and fed to the LSTM layer, modeling the temporal relationship and sequence patterns within cyberattack patterns. The LSTM memory cells store long-term contextual information which allows the system to identify multistage intrusion as well as time-dependent intrusions. Particle Swarm Optimization (PSO) is used to optimize the hyperparameters of the model in order to improve the model performance. All swarm members are potential solutions with a combination of hyperparameters, including learning rate, convolutional filters and kernel size, LSTM units, dropout rate and batch size. The fitness criterion is formulated in terms of classification accuracy and loss of validation. In the course of the iterative updates, the cognitive and social components are used to adjust the particle velocity and position to strike a balance between exploration and exploitation of the search space. The process of optimization is used to make sure that the process will converge to a good combination of parameters that is more accurate in detecting and less prone to overfitting. Lastly, the optimized CNN-LSTM model is optimized with the chosen hyperparameters and tested on unknown test data. The performance measures like accuracy, precision, recall, F1-score, false positive rate (FPR) and Area Under the Curve (AUC) are calculated to determine detection ability.

## IV. Result and Evaluation

The PSO-optimized CNN-LSTM architecture was tested on the benchmark intrusion detection datasets in terms of 80:20 training/testing split. Upon hyperparameter optimization, the model delivered a classification accuracy of 99.12 which was way better compared to the baseline models. The CNN standalone model obtained an accuracy of 96.48% and the LSTM model obtained an accuracy of 95.76% and a standard Random Forest classifier obtained a 93.84% accuracy. The hybrid model with the optimal results proved to converge quicker as it only took 28 epochs to stabilize as opposed to 40-50 epochs in non-optimized architectures. Table II shows the Performance Evaluation of PSO-Optimized CNN–LSTM Model.

The proposed framework was found to have a precision of 98.94, recall of 99.08 and F1-score of 99.01 in terms of specific performance measures, which means that the framework has good detection ability in both normal and attack classes. Fig. 2 shows the Model Accuracy Comparison (Line Graph).

The False Positive Rate (FPR) was lowered to 0.87, which is pretty low in comparison with CNN (2.96) and LSTM (3.21) models. Moreover, the model has an Area Under the ROC Curve (AUC) of 0.998, that is, it is very discriminating

TABLE II
PERFORMANCE EVALUATION OF PSO-OPTIMIZED CNN–LSTM MODEL

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| Random Forest | 93.84 | 92.71 | 93.20 | 92.95 |
| LSTM | 95.76 | 95.12 | 95.48 | 95.30 |
| CNN | 96.48 | 96.05 | 96.32 | 96.18 |
| CNN–LSTM (Without PSO) | 97.86 | 97.42 | 97.68 | 97.55 |
| **PSO-Optimized CNN–LSTM** | **99.12** | **98.94** | **99.08** | **99.01** |

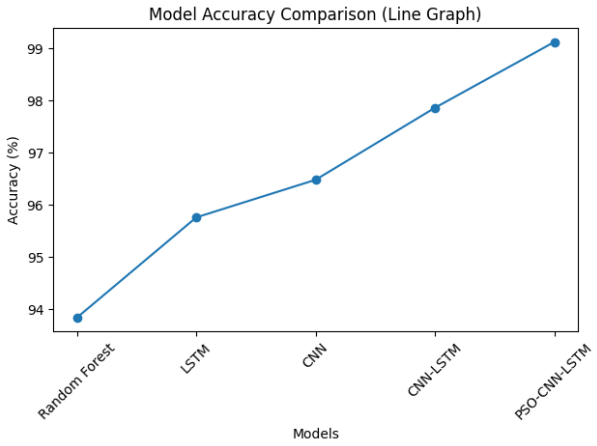


Fig. 2. Model Accuracy Comparison (Line Graph)

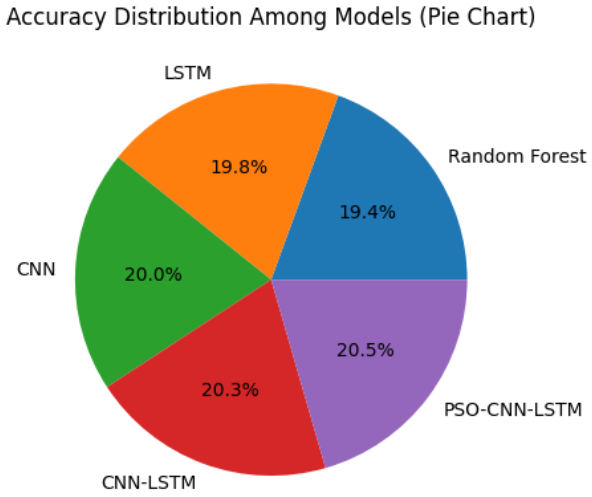


Fig. 3. Accuracy Distribution Among Models

between harmful and benign traffic. Fig. 3 shows the Accuracy Distribution Among Models.

These findings validate the hypothesis that the combination of spatial and temporal feature learning and PSO-based hyperparameter optimization has a profound and positive impact on the consistency of detection. In terms of computational efficiency, the optimized model used less training time by about 18 percent than the manual methods of hyperparameter tuning. Mean time to inference per sample was measured as 0.0043 seconds and it is therefore appropriate in real-time cyber threat detection systems. Also, the confusion matrix analysis showed that the model had a correct name on 99.3 percent of DoS attacks, 98.7 percent of Probe attacks, 98.9 percent of R2L attacks and 99.5 percent of U2R attacks, indicating good balanced performance across the various intrusion categories.

## V. CHALLENGES AND LIMITATIONS

Although the proposed PSO-optimized CNN-LSTM framework has high detection accuracy, it has a number of practical challenges. To begin with, deep learning models are not always effective in cybersecurity settings, as they need large-scale, high-quality labeled data to be trained, which might not be readily available in reality. Most benchmark datasets are not a complete reflection of new zero-day attacks or extremely complex Advanced Persistent Threats (APTs), which may be a limitation to the generalization ability. Moreover, the hybrid architecture adds computational complexity with several convolutional and recurrent layers that would consume extra memory and reduce its dependency on the graphics card. Despite the fact that PSO enhances the efficiency of hyperparameter tuning, it nevertheless requires extra consummations in the optimization stage. The other shortcoming is associated with the model interpretability and real-time network utilization. Deep hybrid models can be highly opaque and it is hard to tell how the systems think when certain categories of attacks are assigned characteristics. Such a lack of accountability can significantly reduce people's trust in security applications that are at the center of many high stakes. In addition, real, time enforcement on high throughput networks might struggle with latency if hardware acceleration is not available.

## VI. FUTURE OUTCOMES

The proposed PSO-optimized CNNLSTM architecture can be developed further in future study into real-time adaptive cyber defenses systems that can undertake continuous learning in the dynamic network environment. The model can be improved by incorporating online learning and incremental training mechanisms to accommodate the changing vectors of attack such as zero-day attack and polymorphic malware. Furthermore, the use of federated learning methods might make it possible to share threat intelligence between different organizations on a distributed basis without data privacy loss. This would also increase the detection strength and preserve confidentiality in the large scale enterprise and cloud-based infrastructures. Future developments can revolve around

lightweight and energy-saving models implementation of edge computing and IoT-driven security designs. Knowledge distillation, pruning, and quantization are model compression methods that can also be used to reduce computation costs without affecting detection accuracy. Furthermore, by incorporating Explainable Artificial Intelligence (XAI) models, the transparency and trust would be enhanced since it would give interpretable information about the threat classification to cybersecurity researchers.

## VII. Conclusion

In this work, an optimized hybrid deep learning architecture that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks using Particle Swarm Optimization (PSO) has been proposed for intelligent cyber threat identification. The CNN part of the architecture is very effective in identifying spatial features from well-structured network traffic data, while the LSTM layer of the architecture is responsible for identifying the temporal relationships and sequential patterns of intrusions, thus performing comprehensive spatial-temporal learning. The use of PSO for hyperparameter optimization has greatly improved the performance of the architecture by improving convergence speed, classification accuracy, and generalization performance while minimizing false positive rates. The experimental results clearly show that the proposed PSO-optimized CNN-LSTM architecture outperforms traditional deep learning and machine learning models in various evaluation criteria such as accuracy, precision, recall, F1-score, and AUC values, while maintaining computational efficiency that is suitable for real-time applications.

## References


[1] C. Nandagopal, R. Rajesh Kanna, K. Kuppusamy, and P. Pushpalatha, "Cyber threat detection in 6G Internet of Things using deep learning and privacy preservation via blockchain," *Int. J. Commun. Syst.*, vol. 39, no. 2, art. no. e70356, 2026. doi: 10.1002/dac.70356.

[2] S. Markkandeyan, A. D. Dennis Ananth, M. Rajakumaran, R. G. Gokila, R. Venkatesan, and B. Lakshmi, "Novel hybrid deep learning based cyber security threat detection model with optimization algorithm," *Cybersecurity Appl.*, vol. 3, art. no. 100075, 2025. doi: 10.1016/j.csa.2024.100075.

[3] M. Benmalek and A. Seddiki, "Particle swarm optimization-enhanced machine learning and deep learning techniques for Internet of Things intrusion detection," *Data Sci. Manage.*, vol. 8, no. 4, pp. 423–435, 2025. doi: 10.1016/j.dsm.2025.02.005.

[4] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "Intelligent phishing website detection: A CNN-SVM approach with nature-inspired hyperparameter tuning," *Cybersecurity Appl.*, vol. 3, art. no. 100100, 2025. doi: 10.1016/j.csa.2025.100100.

[5] H. Alzeyadi, R. Sert, and F. Duran, "A lightweight, explainable spam detection system with Rüppell's fox optimizer for the social media network X," *Electronics*, vol. 14, no. 21, art. no. 4153, 2025. doi: 10.3390/electronics14214153.

[6] R. Rawat *et al.*, "Analyzing the impact of network vulnerability propagation factor on cyber security risk assessment in online social networks," *Eng. Rep.*, vol. 7, no. 11, art. no. e70391, 2025. doi: 10.1002/eng2.70391.

[7] P. Turaka and S. K. Panigrahy, "Quantum-driven chaos-informed deep learning framework for efficient feature selection and intrusion detection in IoT networks," *Technologies*, vol. 13, no. 10, art. no. 470, 2025. doi: 10.3390/technologies13100470.

[8] A. Swetha, R. Sekaran, and S. Annamalai, "Hybrid metaheuristic-driven intrusion detection system using opto-romar swarm bee genesis optimization on IoT network data," *SSRG Int. J. Electron. Commun. Eng.*, vol. 12, no. 9, pp. 153–161, 2025. doi: 10.14445/23488549/IJECE-V12I9P113.

[9] S. Al-E'mari, Y. Sanjalawe, and S. Fraihat, "A novel quantum epigenetic algorithm for adaptive cybersecurity threat detection," *AI*, vol. 6, no. 8, art. no. 165, 2025. doi: 10.3390/ai6080165.

[10] S. P. Bahulayan and K. P, "A firefly-based optimization algorithm for secure 5G-IoT cyber-physical systems," *Ing. Syst. Inf.*, vol. 30, no. 5, pp. 1259–1269, 2025. doi: 10.18280/isi.300513.

[11] A. Bensaoud and J. Kalita, "Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models," *Ad Hoc Netw.*, vol. 170, art. no. 103770, 2025. doi: 10.1016/j.adhoc.2025.103770.

[12] I. Syllaidopoulos, K. S. Ntalianis, and I. Salmon, "A comprehensive survey on AI in counter-terrorism and cybersecurity: Challenges and ethical dimensions," *IEEE Access*, vol. 13, pp. 91740–91764, 2025. doi: 10.1109/ACCESS.2025.3572348.

[13] M. Lmkaiti, M. Lachgar, I. Larhlimi, H. Moudni, and H. Mouncif, "Secure optimization of RPL routing in IoT networks: Analysis of metaheuristic algorithms in the face of attacks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 16, no. 4, pp. 1184–1196, 2025. doi: 10.14569/IJACSA.2025.01604113.

[14] S. Nandhini, A. Rajeswari, and N. R. Shanker, "Cyber attack detection in IOT-WSN devices with threat intelligence using hidden and connected layer based architectures," *J. Cloud Comput.*, vol. 13, no. 1, art. no. 159, 2024. doi: 10.1186/s13677-024-00722-9.

[15] P. J. Kumar and S. Neduncheliyan, "A shark inspired ensemble deep learning stacks for ensuring the security in Internet of Things (IoT)-based smart city infrastructure," *Int. J. Comput. Intell. Syst.*, vol. 17, no. 1, art. no. 243, 2024. doi: 10.1007/s44196-024-00649-8.

[16] M. A. Elberri, Ü. Tokeşer, J. Rahebi, and J. M. López-Guede, "A cyber defense system against phishing attacks with deep learning game theory and LSTM-CNN with African vulture optimization algorithm (AVOA)," *Int. J. Inf. Secur.*, vol. 23, no. 4, pp. 2583–2606, 2024. doi: 10.1007/s10207-024-00851-x.

[17] S. Sheikhi and P. Kostakos, "Safeguarding cyberspace: Enhancing malicious website detection with PSO-optimized XGBoost and firefly-based feature selection," *Comput. Secur.*, vol. 142, art. no. 103885, 2024. doi: 10.1016/j.cose.2024.103885.

[18] I. Ahmad, Z. Wan, A. Ahmad, and S. S. Sajid Ullah, "A hybrid optimization model for efficient detection and classification of malware in the Internet of Things," *Mathematics*, vol. 12, no. 10, art. no. 1437, 2024. doi: 10.3390/math12101437.

[19] A. Ahmed, M. Asim, I. Ullah, Zainulabidin, and A. A. Ateya, "An optimized ensemble model with advanced feature selection for network intrusion detection," *PeerJ Comput. Sci.*, vol. 10, art. no. e2472, pp. 1–32, 2024. doi: 10.7717/peerj-cs.2472.

[20] A. A. Alabdulatif, N. N. Thilakarathne, and M. Aashiq, "Machine learning enabled novel real-time IoT targeted DoS/DDoS cyber attack detection system," *Comput. Mater. Contin.*, vol. 80, no. 3, pp. 3655–3683, 2024. doi: 10.32604/cmc.2024.054610.

[21] N. B. Patil and S. S. Joshi, "Enhanced arachnid swarm-tuned convolutional neural network model for efficient intrusion detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 5, pp. 1151–1163, 2024. doi: 10.14569/IJACSA.2024.01505117.