An Intelligent Cybersecurity Framework for IoT Environments Using a Multi-Stage Heuristic Algorithm Fused with a Spatiotemporal Attention Mechanism

Hassan A. Alterazi

Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
haalterazi@kau.edu.sa (corresponding author)

Received: 4 November 2025 | Revised: 6 December 2025 and 11 December 2025 | Accepted: 13 December 2025

 DOI: https://doi.org/10.48084/etasr.16005

ABSTRACT

With the increasing risk of cyberattacks, cybersecurity has now become a major area of the Internet of Things (IoT). Cyberattacks on IoT devices can result in serious concerns, including unauthorized access, disruption of critical services, and data breaches. IoT security aims to decrease the risk for enterprises and users by ensuring the safety of IoT resources and user privacy. Novel cybersecurity tools and technologies have enabled significant improvements in IoT security management. Recently, Artificial Intelligence (AI) has been applied to identify cyber threats, rapidly analyze millions of events, and detect multiple threats. Deep Learning (DL) has proven effective and offers several advantages for addressing IoT cybersecurity challenges. This study proposes an Optimized Dimensionality Reduction with an Attention Mechanism for Cyberattack Detection using Metaheuristic Optimization Algorithms (ODRAMCD-MOA). First, a min–max normalization model is used in the data preprocessing phase. Next, the Fruit Fly Optimization Algorithm (FOA) is employed for Feature Selection (FS). Subsequently, a hybrid of a Convolutional Neural Network (CNN) and a Bidirectional Long Short-Term Memory (BiLSTM) model with a Spatiotemporal Attention (STA) mechanism (CNN-BiLSTM-STA) is utilized for cybersecurity classification. Finally, the hyperparameters of the CNN-BiLSTM-STA method are optimized using the Augmented Red Panda Optimizer (ARPO). Comparative analysis shows that the ODRAMCD-MOA methodology achieves accuracy values of 99.79% and 99.03% on the ToN-IoT and BoT-IoT datasets, respectively, outperforming existing models.

Keywords-cyberattack detection; metaheuristic optimization algorithms; Internet of Things (IoT); attention mechanism; cybersecurity

I. INTRODUCTION

The Internet of Things (IoT) is booming and has become an integral part of everyday lives in various businesses and homes. IoT is difficult to describe because it has been constantly evolving since its inception, but it can be understood as a digital network of computing devices and analog machines supplied with unique identifiers, capable of exchanging data without human intervention [1]. Generally, it involves a human interfacing with an application or central hub device, often a mobile app, which sends instructions and data to one or more edge IoT devices [2]. The edge devices can perform a wide range of functions and transmit data back to the application or hub device for human review [3]. Nevertheless, IoT systems are vulnerable to cyber challenges due to the integration of multiple attack surfaces, their novelty, and the lack of standardized security requirements [4]. A wide range of cyber threats can be exploited by attackers, depending on the targeted system features and the information they aim to obtain [5]. Denial-of-service (DoS) attacks are among the common forms of data intrusion threats [6]. Advanced Intrusion Detection Systems (IDSs) rely heavily on the ability to distinguish abnormal from normal data [7]. Deep Learning (DL) methods, including Long Short-Term Memory (LSTM), are widely used in malware detection, fraud detection, and image analysis [8], and are responsible for many recent advancements in IoT cybersecurity.

Authors in [9] presented a novel unified Quantum-Resilient BC-Zero-Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF) methodology, utilizing Hybrid Reinforcement-Lattice Blockchain Key Generation (Hybrid RL-Lattice KeyGen), Deep Q-Network Multi-Factor Secure Key (DQN-MFSK) selection, and Zero-Knowledge Proofs (ZKP). Authors in [10] utilized Stacked Long Short-Term Memory (SLSTM) networks and Willow Catkin Optimization (WCO). Authors in [11] employed Scenario-Based Simulations (SBS), Synthetic Data Generation (SDG), Threat Modeling

(TM), and Discrete-Event Simulation (DES). Authors in [12] utilized Software-Defined Network (SDN) micro-segmentation, a centralized Security Management Layer (SML), and asynchronous policy distribution. Authors in [13] presented the IIoT-IDFE method using Federated Learning (FL) and Ensemble Learning (EL) through the Shared Local Ensemble (SLE) and Broadcast Global Ensemble (BGE) models. Authors in [14] utilized a basic Autoencoder (bAE) for dimensionality reduction, deep Autoencoder (dAE) and One-Class Support Vector Machine (OCSVM) for anomaly detection, and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) for attack clustering. Authors in [15] enhanced IoT network security by utilizing Fog Node Data Analysis (FNDA), Local Anomaly Detection (LAD), Machine Learning (ML), and Ensemble Classification Integration (ECI). Authors in [16] utilized Blockchain (BC) and AI-based metaheuristic algorithms for efficient offloading decisions. Authors in [17] improved network intrusion detection using Parallel Multi-Scale Convolution (PMSC), Bidirectional Temporal Attention (BTA) with residual-enhanced LSTM, and a Packet-Level Transformer (PLT). Authors in [18] improved IoT network security using Sliding Window Sampling (SWS), Nonlinear Feature Transformation (NFT), and EdgeNet with Depthwise Separable Convolution (DSC) and Self-Attention Mechanism (SAM). Table I summarizes the referenced studies.

This study proposes the Optimized Dimensionality Reduction with an Attention Mechanism for Cyberattack Detection using Metaheuristic Optimization Algorithms (ODRAMCD-MOA). The methodology consists of the following steps:

- Initially, min–max normalization is applied for improved feature scaling, followed by the Fruit Fly Optimization Algorithm (FOA) for Feature Selection (FS) to detect the most relevant features, reducing dimensionality and improving model efficiency.
- Next, spatial and temporal patterns are integrated using a hybrid of a Convolutional Neural Network (CNN) and a Bidirectional Long Short-Term Memory (BiLSTM) model with a Spatiotemporal Attention (STA) mechanism (CNN-BiLSTM-STA) for accurate cybersecurity threat detection.
- Finally, hyperparameters are optimized using the Augmented Red Panda Optimizer (ARPO) to maximize classification performance.

The novelty of the proposed method lies in the integration of CNN-BiLSTM with STA and ARPO-based tuning, providing a robust and highly accurate cybersecurity classification framework.

TABLE I. SUMMARY OF EXISTING STUDIES ON CYBERSECURITY FRAMEWORKS FOR IOT ENVIRONMENTS

Reference	Objective	Method	Dataset	Measures
[9]	Develop a framework for secure identity and access management in IoT	QBC-ZKPAF, Hybrid RL-Lattice KeyGen, DQN-MFSK, ZKP	Edge-IIoTset cyber security dataset	Privacy: 98%, Throughput: 700 TPS, Energy: 0.7 J, Quantum Resilience: 98%
[10]	Develop an efficient intrusion-detection model for IoT networks	SLSTM, WCO	BoT-IoT, IoT-23, MQTT, MQTTset	Accuracy: 99.49%
[11]	Develop a lightweight dynamic risk assessment model to identify and mitigate cybersecurity threats	SBS, SDG, TM, DES	Synthetic MIoT data and threat models	High threat detection
[12]	Design a resilient and flexible security architecture for Industrial IoT (IIoT) systems	SDN, SML	Prototype IIoT network simulation	High resilience
[13]	Develop a privacy-preserving and efficient intrusion-detection model	IIoT-IDFE, FL, EL, SLE, BGE	Edge-IIoTset, ToN-IoT	Accuracy: 99.99–100%
[14]	Develop a model to detect novel attacks efficiently	bAE, dAE, OCSVM, DBSCAN	CIC-IDS2017, CSECIC-IDS2018	Accuracy: >98%
[15]	Develop a method to detect and mitigate cyberattacks in real-time	FNDA, LAD, ML, ECI	NSL-KDD	Accuracy: 99.80%, Precision: 99.85%, Recall: 99.70%, F1-score: 99.77%, False alarm: 0.74%
[16]	Optimize resource allocation and enhance security for latency-sensitive IoT applications	BC, AI	Simulated IoT workload data	Execution time: –20% Energy consumption: –18%, Cost: –20%
[17]	Improve network intrusion detection using a hierarchical DL model	PMSC, BTA, residual-enhanced LSTM, PLT	NSL-KDD, UNSW-NB15, CIC-DDoS2019	Accuracy: 86–99.69%
[18]	Develop a lightweight, real-time IDS	SWS, NFT, EdgeNet with DSC, SAM	IoT network traffic data	High classification accuracy

II. MATERIALS AND METHODS

This study presents the ODRAMCD-MOA method, which comprises multiple stages, including data preprocessing, FS, classification, and parameter tuning. Figure 1 illustrates the overall workflow of the ODRAMCD-MOA method.

A. Data Preprocessing

Initially, the min–max normalization system is applied to transform input data into a suitable range. Min–max normalization is a commonly applied data preprocessing approach in cybersecurity for IoT systems, scaling numeric attributes within a predefined range, typically [0,1] or [-1,1]. It

guarantees that each input feature contributes appropriately to threat detection methods, preventing features with larger magnitudes from dominating the analysis [19]. This model is particularly helpful in IoT environments, where sensor data, network traffic, and security logs differ considerably in scale. By using min–max normalization, ML methods attain quicker convergence, improved precision and anomaly detection capabilities. It also improves the robustness of IDSs by decreasing bias produced by variable data distributions. Moreover, within a metaheuristic-optimized threat detection framework, min–max normalization enhances FS efficacy, resulting in more consistent cybersecurity solutions.

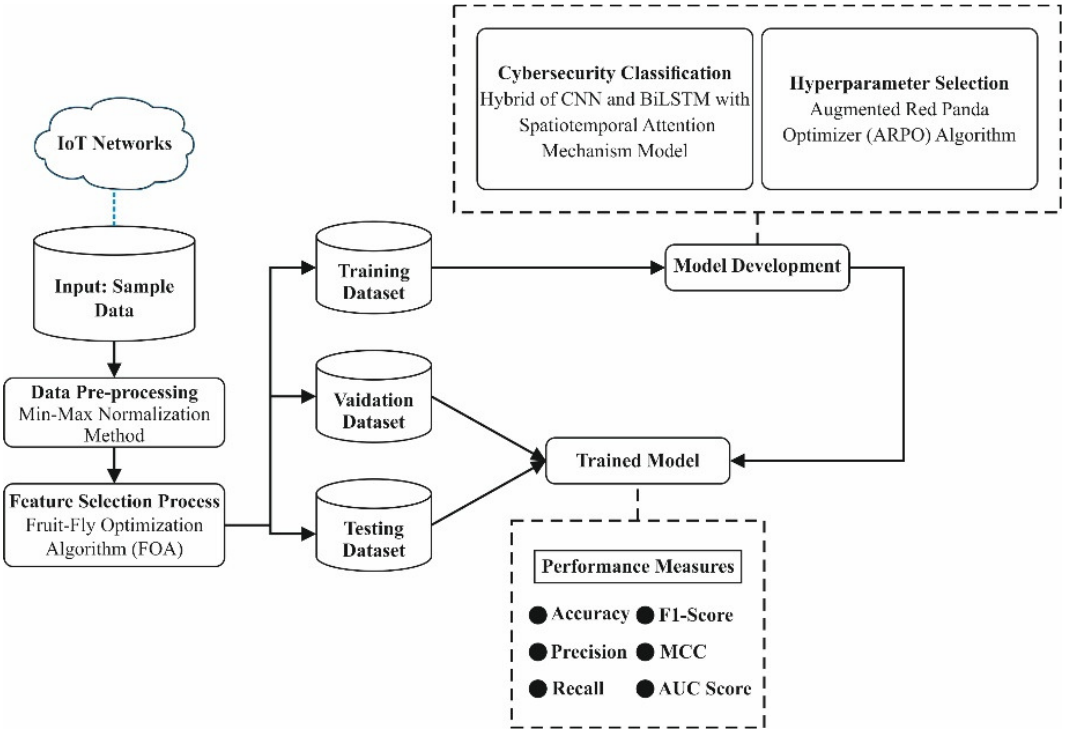

Fig. 1. Workflow of the ODRAMCD-MOA method.

B. Fruit Fly Optimization Algorithm–Based Feature Selection Process

In this step, the FOA is used for the FS process to identify the most relevant features from the input dataset. The algorithm simulates the feeding behavior of fruit flies, which use their visual and olfactory senses to locate food more efficiently than other species [20]. The key steps mimic Drosophila behavior: primarily, fruit flies use their olfactory organs to identify the existence of food and then fly in that direction. Subsequently, swarms of fruit flies continuously search the surrounding area. The FOA starts by randomly initializing the locations of the Drosophila colony along the X and Y axes, as indicated in (1) and (2):

$$Init\ X\_axis = rands(1,2) \quad (1)$$

$$Init\ Y\_axis = rands(1,2) \quad (2)$$

Each fruit fly moves in arbitrary directions and distances to explore the environment using its sense of smell. The distance from the resource is calculated using (3) and (4):

$$Dist_i = \sqrt{X_i^2 + Y_i^2} \quad (3)$$

$$S_i = \frac{1}{Dist_i} \quad (4)$$

A Fitness Function (FF) is used to compute the taste concentration ($Smell_i$), and the fruit fly with the best taste value is detected. The population then moves toward the optimal position by updating its coordinates. The steps of movement, evaluation, and updating are iteratively repeated until the taste concentration cannot be further improved, ensuring convergence to the optimal solution.

In FOA, the FF balances the proposed attributes in all solutions (least) and the classifier precision (highest) achieved through the selected features, Equation (5) defines the FF for approximating the optimal solution:

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|} \quad (5)$$

where $\gamma_R(D)$ symbolizes the classification error rate of the given classifier, $|R|$ denotes the cardinality of the selected feature subset, and $|C|$ the total number of features in the dataset. The parameters α and β control the relative importance of feature subset size and classification quality, respectively.

C. CNN-BiLSTM-STA-Based Classification Process

Next, the CNN-BiLSTM-STA approach is used for cybersecurity classification. CNNs act as the initial step to extract spatial features from the input data [21]. Primarily, two CNN layers carry out convolutional processes, which inspect

local receptive areas to recognize spatial patterns. In such cases, the traditional process is expressed in (6):

$$z_{i,j,k} = \sigma\left(\sum_{m,n} x_{m,n} w_{i,j,m,n} + b_k\right) \quad (6)$$

The dual CNN layer is applied on all frames of the input sequence, and the extracted spatial features serve as input to the spatiotemporal attention mechanism, which concentrates on crucial temporal segments and spatial regions. Spatial attention is computed using (7):

$$SA_t = \sigma(Conv2D(x_t, W_s) + b_s) \quad (7)$$

The resulting spatial scores are then refined using temporal attention to determine temporal importance, as shown in (8).

$$TA_t = \sigma(Dense(Flatten(S_t), W_t) + b_t) \quad (8)$$

Equation (9) computes the Hadamard product, and the resulting features are processed through a third CNN layer to enhance feature representation. The output is then sent to BiLSTM layers [22] for forward and backward temporal modeling, followed by normalization, a second BiLSTM layer, and finally a dense decoding layer for classification, as specified in (10):

$$CA_t = SA_t \odot TA_t \quad (9)$$

$$Prediction = Reshape(Dense(y_i, W_o) + b_o) \quad (10)$$

where W_o signifies the output-layer weights and b_o denotes the bias term.

D. Augmented Red Panda Optimizer–Based Hyperparameter Tuning Model

Finally, the hyperparameter tuning of the CNN-BiLSTM-STA model is executed using the ARPO model. The Particle Swarm Optimization (PSO) model is a robust metaheuristic approach in which each particle's movement is influenced by its own experience and the global state of the swarm. While the Red Panda Optimizer (RPO) [23] is a nature-inspired optimization algorithm that simulates the searching behavior of red pandas during the exploration of optimal solutions, the objective of incorporating PSO principles is to enhance the convergence speed and exploration capability of RPO. The ARPO model combines RPO with PSO, retaining RPO's adaptive search strategy while benefiting from the position update mechanisms of PSO. It begins by clustering red pandas with random positions and velocities, and tracking the personal best ($pbest$) and global best ($gbest$) solutions, The agents update their velocities and positions based on the current velocity, cognitive (c_1), and social (c_2) components. The velocity and position updates are defined by (11) and (12):

$$v_i = w \times v_i + c_1 \times rand \times (p_{best} - Y_i) + c_2 \times rand \times (g_{best} - Y_i) \quad (11)$$

$$Y_i = Y_i + v_i \quad (12)$$

Here, w denotes the inertia weight, and c_1 and c_2 represent the acceleration coefficients. Randomness is introduced using the $rand$ function. The FF guides the optimization process. In the proposed ARPO model, precision is selected as the primary optimization objective and is defined as follows:

$$Fitness = \max(P) \quad (13)$$

$$P = \frac{TP}{TP+FP} \quad (14)$$

Here, TP and FP represent the true positive and false positive values, respectively.

III. EXPERIMENTAL ANALYSIS

The experimental validation of the ODRAMCD-MOA model is conducted on the ToN-IoT dataset [24] and BoT-IoT dataset [25]. The method runs on Python 3.6.5 with an Intel Core i5-8600k CPU, 4 GB GPU, 16 GB RAM, 250 GB SSD, and 1 TB HDD. The model is trained using a learning rate of 0.01, ReLU activation, 50 epochs, 0.5 dropout, and a batch size 5. The ToN-IoT dataset comprises a total of 119,957 instances across ten classes, including normal traffic (78,369) and various cyberattacks, such as Man-in-The-Middle (MiTM) (336), DoS (5,440), Distributed DoS (DDoS) (5,987), password attacks (6,016), injection (5,867), Cross-Site Scripting (XSS) (5,951), ransomware (5,976), and backdoor (6,015). There are 42 attributes in this dataset, but only 29 attributes are chosen. The dataset was chosen for its realistic and heterogeneous IoT telemetry, and its high-quality labeled botnet attack traffic, providing broader attack diversity and enabling a more comprehensive evaluation than other IoT cybersecurity datasets.

Figure 2 illustrates the confusion matrices generated by the ODRAMCD-MOA approach on the ToN-IoT dataset under 80:20 and 70:30 training/testing (TRAPS/TESPS) splits. The findings indicate that the ODRAMCD-MOA model accurately identifies and classifies all attack categories.

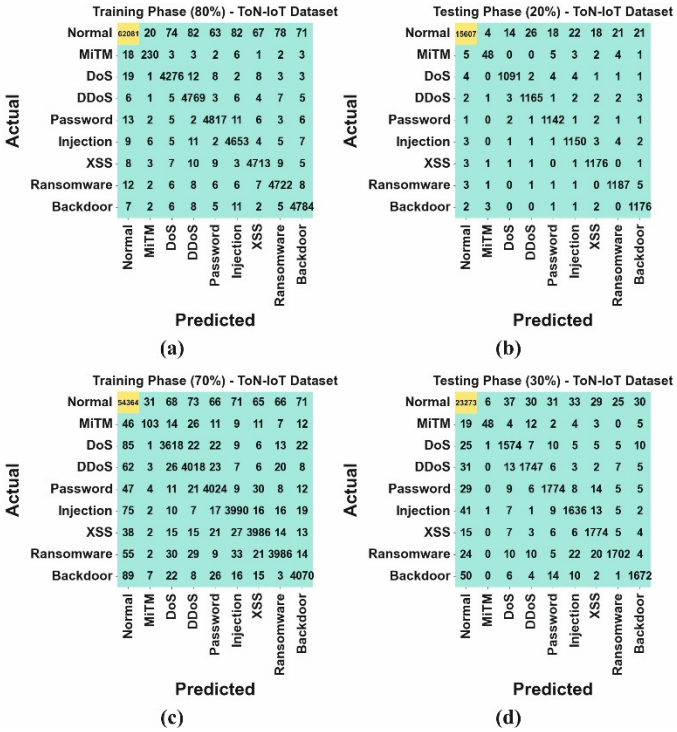

Fig. 2. Confusion matrices for the ToN-IoT dataset: (a) training (80:20 TRAPS/TESPS), (b) testing (80:20 TRAPS/TESPS), (c) training (70:30 TRAPS/TESPS), and (d) testing (70:30 TRAPS/TESPS).

The comparison study of the ODRAMCD-MOA method on the ToN-IoT dataset against recent techniques is presented in Table II [26, 27]. In terms of $accu_y$, the ODRAMCD-MOA method achieves a superior value of 99.79%, whereas the Artificial Neural Network (ANN), Trustworthy Privacy-Preserving Secured Framework (TP2SF), Densely-ResNet, Deep Feedforward (DFF), Extreme Gradient Boosting (XGBoost), Inception Time (IT), and Naïve Bayes (NB) approaches achieve lower $accu_y$ of 99.44%, 98.84%, 92.99%, 97.35%, 98.30%, 98.30%, and 96.78%, respectively.

TABLE II. COMPARISON OF THE ODRAMCD-MOA APPROACH ON THE TON-IOT DATASET

Method	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$
ANN method [26]	99.44	90.56	93.04	94.54
TP2SF [26]	98.84	94.67	92.54	96.05
Densely-ResNet [26]	92.99	93.00	93.31	95.17
DFF model [26]	97.35	94.87	91.42	90.40
XGBoost [27]	98.30	95.75	91.55	92.68
IT [27]	98.30	90.44	92.35	93.96
NB [27]	96.78	90.56	92.25	92.95
ODRAMCD-MOA [proposed]	99.79	96.61	97.52	97.06

Similarly, the ODRAMCD-MOA method is evaluated on the BoT-IoT dataset [25], containing 2,056 instances across five classes: DDoS (500), DoS (500), Reconnaissance (Recon) (500), theft (79), and normal (477). Of the 34 features, 26 are selected for training and evaluating IoT IDSs. Figure 3 depicts the confusion matrices of the ODRAMCD-MOA method on the BoT-IoT dataset under 80:20 and 70:30 TRAPS/TESPS splits. The findings imply that the ODRAMCD-MOA model successfully identifies all attack classes.

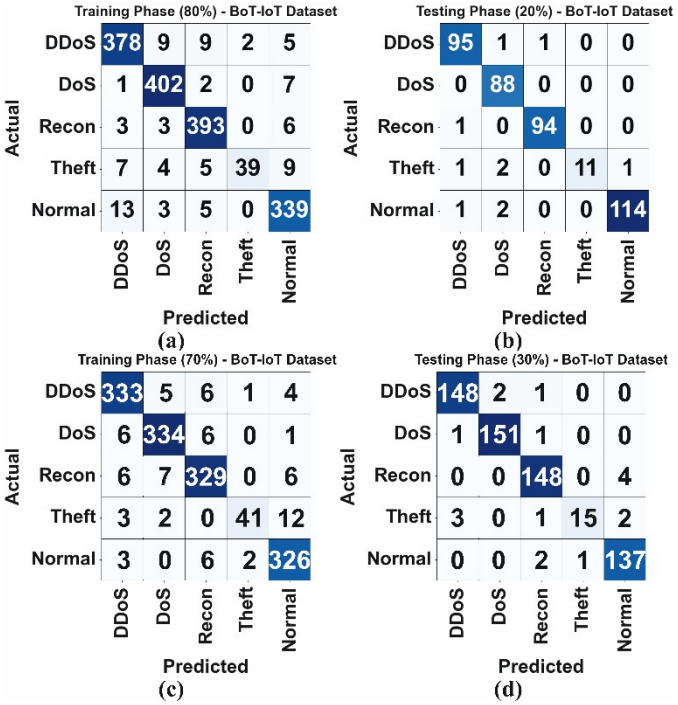

Fig. 3. Confusion matrices for the BoT-IoT dataset: (a) training (80:20 TRAPS/TESPS), (b) testing (80:20 TRAPS/TESPS), (c) training (70:30 TRAPS/TESPS), and (d) testing (70:30 TRAPS/TESPS).

Table III presents the comparison study of the ODRAMCD-MOA approach against existing methods on the BoT-IoT dataset [26, 27]. The ODRAMCD-MOA model achieves the highest performance, with $accu_y$, $prec_n$, $reca_l$, and $F1_{score}$ values of 99.03%, 97.93%, 93.53%, and 95.30%, respectively. In contrast, the Harris Hawks with Sine Cosine and a Deep Learning-based Intrusion Detection System (H3SC-DLIDS), Autoencoder–Multilayer Perceptron (AE-MLP), IDS-IoT, InceptionV3, XGBoost, Random Forest (RF), and Decision Tree (DT) models exhibit lower performance.

TABLE III. COMPARISON OF THE ODRAMCD-MOA APPROACH ON THE BOT-IOT DATASET

Method	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$
ODRAMCD-MOA [proposed]	99.03	97.93	93.53	95.30
H3SC-DLIDS [27]	98.81	96.71	90.44	93.63
AE-MLP model [27]	98.19	95.96	92.50	92.50
IDS-IoT model [27]	97.40	95.86	91.33	90.04
XGBoost model [27]	97.09	94.34	90.71	89.98
RF method [26]	97.00	95.03	92.89	91.21
DT classifier [26]	95.21	92.50	89.71	92.81

IV. CONCLUSION

This paper presents the Optimized Dimensionality Reduction with Attention Mechanism for Cyberattack Detection using Metaheuristic Optimization Algorithms (ODRAMCD-MOA) method as an effective threat detection framework for Internet of Things (IoT) networks, leveraging cutting-edge optimization techniques to enhance cybersecurity. Initially, the min–max normalization technique is applied in the data preprocessing phase. Next, the Fruit Fly Optimization Algorithm (FOA) is deployed for Feature Selection (FS). A hybrid of Convolutional Neural Network (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) with Spatiotemporal Attention Mechanism (STA) (CNN-BiLSTM-STA) is then used for cybersecurity classification. Finally, the hyperparameter tuning of the CNN-BiLSTM-STA model is performed using the Augmented Red Panda Optimizer (ARPO). The comparative analysis demonstrates that the ODRAMCD-MOA methodology achieves superior accuracy, with 99.79% and 99.03% on the ToN-IoT and BoT-IoT datasets, respectively, outperforming other existing models.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are openly available at: https://www.kaggle.com/datasets/dhoogla/cictoniot, and https://research.unsw.edu.au/projects/bot-iot-dataset.

REFERENCES

[1] O. Aouedi *et al.*, "A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 2, pp. 1238–1292, Apr. 2025, https://doi.org/10.1109/COMST.2024.3430368.

[2] J. Shehu Yalli, M. Hilmi Hasan, and A. Abubakar Badawi, "Internet of Things (IoT): Origins, Embedded Technologies, Smart Applications, and Its Growth in the Last Decade," *IEEE Access*, vol. 12, pp. 91357–91382, 2024, https://doi.org/10.1109/ACCESS.2024.3418995.

[3] N. U. Prince, M. A. A. Mamun, A. O. Olajide, O. U. Khan, A. B. Akeem, and A. I. Sani, "IEEE Standards and Deep Learning Techniques

for Securing Internet of Things (IoT) Devices Against Cyber Attacks," *Journal of Computational Analysis and Applications*, vol. 33, no. 7, pp. 1270–1289, Sept. 2024.

[4] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Towards a Lightweight Detection System for Cyber Attacks in the IoT Environment Using Corresponding Features," *Electronics*, vol. 9, no. 1, Jan. 2020, Art. no. 144, https://doi.org/10.3390/electronics9010144.

[5] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions," *Electronics*, vol. 11, no. 20, Oct. 2022, Art. no. 3330, https://doi.org/10.3390/electronics11203330.

[6] M. M. Abualhaj, S. N. Al-Khatib, M. A. Zyoud, I. Qaddara, and M. Anbar, "Enhancing Intrusion Detection System Performance Using a Hybrid of Harris Hawks and Whale Optimization Algorithms," *Engineering, Technology & Applied Science Research*, vol. 15, no. 4, pp. 24354–24361, Aug. 2025, https://doi.org/10.48084/etasr.10919.

[7] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey," *Electronics*, vol. 11, no. 1, Jan. 2022, Art. no. 16, https://doi.org/10.3390/electronics11010016.

[8] A. A. A. Mohammed, "Improving Intrusion Detection Systems by Using Deep Learning Methods on Time Series Data," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19267–19272, Feb. 2025, https://doi.org/10.48084/etasr.9417.

[9] M. A. Aleisa, "Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments," *IEEE Access*, vol. 13, pp. 18660–18676, 2025, https://doi.org/10.1109/ACCESS.2025.3529309.

[10] T. Sharma and S. K. Prasad, "Enhancing cybersecurity in IoT networks: SLSTM-WCO algorithm for anomaly detection," *Peer-to-Peer Networking and Applications*, vol. 17, no. 4, pp. 2237–2258, July 2024, https://doi.org/10.1007/s12083-024-01712-z.

[11] R. M. Czekster, T. Webber, L. B. Furstenau, and C. Marcon, "Dynamic risk assessment approach for analysing cyber security events in medical IoT networks," *Internet of Things*, vol. 29, Jan. 2025, Art. no. 101437, https://doi.org/10.1016/j.iot.2024.101437.

[12] C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," *Ad Hoc Networks*, vol. 156, Apr. 2024, Art. no. 103414, https://doi.org/10.1016/j.adhoc.2024.103414.

[13] A. Chahal, P. Gulia, N. S. Gill, and D. Rani, "Design of a federated ensemble model for intrusion detection in distributed IIoT networks for enhancing cybersecurity," *Journal of Industrial Information Integration*, vol. 44, Mar. 2025, Art. no. 100800, https://doi.org/10.1016/j.jii.2025.100800.

[14] P. Kaliyaperumal, S. Periyasamy, M. Thirumalaisamy, B. Balusamy, and F. Benedetto, "A Novel Hybrid Unsupervised Learning Approach for Enhanced Cybersecurity in the IoT," *Future Internet*, vol. 16, no. 7, July 2024, Art. no. 253, https://doi.org/10.3390/fi16070253.

[15] M. Aknan, M. P. Singh, and R. Arya, "Secure Cloud Assisted Fog Computing Framework for IoT Applications Using Ensemble Learning," *SN Computer Science*, vol. 6, no. 6, Aug. 2025, Art. no. 717, https://doi.org/10.1007/s42979-025-04257-x.

[16] M. Aknan, M. P. Singh, and R. Arya, "AI and Blockchain Assisted Framework for Offloading and Resource Allocation in Fog Computing," *Journal of Grid Computing*, vol. 21, no. 4, Nov. 2023, Art. no. 74, https://doi.org/10.1007/s10723-023-09694-7.

[17] X. Yang, Y. Cui, and H. Li, "M3NID: an intrusion detection system based on the dual-mode spatio-temporal feature fusion method," *PeerJ Computer Science*, vol. 11, Nov. 2025, Art. no. e3393, https://doi.org/10.7717/peerj-cs.3393.

[18] X. Kong, Y. Zhou, Y. Xiao, X. Ye, H. Qi, and X. Liu, "iDetector: A Novel Real-Time Intrusion Detection Solution for IoT Networks," *IEEE Internet of Things Journal*, vol. 11, no. 19, pp. 31153–31166, Oct. 2024, https://doi.org/10.1109/JIOT.2024.3416746.

[19] P. Muhammad Ali and R. Faraj, "Data Normalization and Standardization: A Technical Report," *Machine Learning Technical Reports*, vol. 1, no. 1, pp. 1–6, Jan. 2014, https://doi.org/10.13140/RG.2.2.28948.04489.

[20] H. Iscan and M. Gunduz, "A Survey on Fruit Fly Optimization Algorithm," in *2015 11th International Conference on Signal-Image Technology & Internet-Based Systems*, Bangkok, Thailand, 2015, pp. 520–527, https://doi.org/10.1109/SITIS.2015.55.

[21] C. Zhou, C. Sun, Z. Liu, and F. C. M. Lau, "A C-LSTM Neural Network for Text Classification." arXiv, Nov. 30, 2015, https://doi.org/10.48550/arXiv.1511.08630.

[22] F. Karim, S. Majumdar, H. Darabi, and S. Harford, "Multivariate LSTM-FCNs for time series classification," *Neural Networks*, vol. 116, pp. 237–245, Aug. 2019, https://doi.org/10.1016/j.neunet.2019.04.014.

[23] H. Givi, M. Dehghani, and Š. Hubálovský, "Red Panda Optimization Algorithm: An Effective Bio-Inspired Metaheuristic Algorithm for Solving Engineering Optimization Problems," *IEEE Access*, vol. 11, pp. 57203–57227, 2023, https://doi.org/10.1109/ACCESS.2023.3283422.

[24] M. Sarhan, "CIC-ToN-IoT." Kaggle. [Online]. Available: https://www.kaggle.com/datasets/dhoogla/cictoniot.

[25] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on Machine Learning Techniques," in *International Conference on Mobile Networks and Management*, Melbourne, Australia, 2017, pp. 30–44, https://doi.org/10.1007/978-3-319-90775-8_3.

[26] I. Tareq, B. M. Elbagoury, S. El-Regaily, and E.-S. M. El-Horbaty, "Analysis of ToN-IoT, UNW-NB15, and Edge-IIoT Datasets Using DL in Cybersecurity for IoT," *Applied Sciences*, vol. 12, no. 19, Oct. 2022, Art. no. 9572, https://doi.org/10.3390/app12199572.

[27] I. Katib and M. Ragab, "Blockchain-Assisted Hybrid Harris Hawks Optimization Based Deep DDoS Attack Detection in the IoT Environment," *Mathematics*, vol. 11, no. 8, Apr. 2023, Art. no. 1887, https://doi.org/10.3390/math11081887.