INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Enhancing IoT Security through Machine Learning-Based Intrusion Detection Systems

Monali B Suthar[1]*, **Satvik Khara**[1]

1 Silver Oak University, Ahmedabad, Gujarat, India

OPEN ACCESS

Received: 12/04/2025

Accepted: 15/08/2025

Published: 29/09/2025

Citation: Suthar MB, Khara S (2025) Enhancing IoT Security through Machine Learning-Based Intrusion Detection Systems. Indian Journal of Science and Technology 18(35): 2884-2896. https://doi.org/10.17485/IJST/v18i35.684

* **Corresponding author**.

monalisuthar.rs@silveroakuni.ac.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: This study targets the pressing limitations of traditional Intrusion Detection Systems (IDS) in IoT environments, notably the challenges posed by high-dimensional data, fluctuating detection accuracy, and elevated false alarm rates. **Method:** This study proposes a hybrid intrusion detection model that combines Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC), and Deep Convolutional Neural Networks (DCNN). PSO and ABC are utilized for optimized feature selection, while DCNN performs hierarchical anomaly classification. The model is trained and evaluated on the UNSW-NB15 dataset, a widely accepted IoT intrusion benchmark. **Findings:** The proposed PSO-ABC-DCNN model achieves an accuracy of 99.41%**,** significantly outperforming existing models such as CNN (92.8%) and LSTM (98.2%). **Novelty:** The novelty lies in the integrated use of swarm intelligence techniques (PSO and ABC) with deep learning to create a lightweight, high-performance IDS. This synergistic approach enhances feature optimization, model generalization, and scalability in complex IoT environments.

Keywords: IoT; Intrusion Detection; Machine Learning; Security; Cybersecurity; Supervised Learning; Unsupervised Learning; Deep Learning; Bot-IoT; UNSW-NB 15

1 Introduction

The rapid evolution of the Internet of Things (IoT) has transformed critical sectors such as healthcare, manufacturing, agriculture, and transportation by enabling interconnected devices to generate massive volumes of real-time data. While this has enhanced operational efficiency, the decentralized and resource-constrained nature of IoT systems introduces serious security vulnerabilities. Devices with minimal hardware protection and limited computational resources are often targeted for cyberattacks such as unauthorized access, denial-of-service (DoS), and data exfiltration [(1)], [(2)].

To counter these threats, researchers have developed intrusion detection systems (IDS) tailored for IoT networks. Traditional signature-based IDS tools like Snort and Suricata are limited by their inability to detect novel or zero-day attacks. As a result, recent efforts have shifted toward machine learning (ML) and deep learning (DL)-based IDS to detect previously unseen threats [(3)], [(4)]. However, several limitations still

persist. Many ML and DL approaches lack scalability, generalizability across datasets, and robustness against high-dimensional and imbalanced data [5], [6], [7].

The proliferation of Internet of Things (IoT) devices across sectors such as healthcare, manufacturing, and transportation has introduced significant security risks due to their resource constraints and continuous connectivity. Traditional Intrusion Detection Systems (IDS) struggle in these settings due to their inability to adapt to evolving threats, high-dimensional traffic data, and limited computational resources. This has necessitated the development of intelligent IDS models leveraging deep learning and optimization techniques.

In contrast to prior models that rely on fixed architectures or single-phase learning, the novelty of this work lies in its synergistic use of swarm intelligence with deep learning, enabling adaptive, lightweight, and generalizable detection in diverse IoT environments.

Recent breakthrough studies from 2023 to 2025 have attempted to address these challenges using hybrid and deep learning-based models:

- Guerin et al. (2024) [8] employed a CNN-LSTM model that demonstrated improved accuracy in temporal-spatial analysis but required high computational power and complex preprocessing.
- Khairullah & Alsenani (2025) [9] integrated SMOTE with deep neural networks to handle class imbalance, but their models exhibited high training overhead.
- Abdulkareem (2025) [10] proposed a hybrid DL-metaheuristic IDS model but lacked robustness when tested across heterogeneous datasets.
- Yaras & Dener (2024) [11] introduced a new deep hybrid model for anomaly detection but did not optimize for lightweight IoT deployment.

While these approaches demonstrate high accuracy in controlled settings, they are often computationally expensive, susceptible to overfitting, or fail to generalize across real-world traffic.

This study addresses these limitations by proposing a hybrid IDS framework that combines Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC), and Deep Convolutional Neural Networks (DCNN). PSO and ABC optimize feature selection and model parameters, while DCNN facilitates hierarchical feature extraction. The goal is to enhance detection performance while ensuring the system remains lightweight and adaptable for IoT scenarios.

Objective:

The primary objective of this research is to enhance intrusion detection in IoT environments using a hybrid deep learning model combining DNN, PSO, and ABC algorithms. The specific goals are:

1. To design an effective intrusion detection system tailored for IoT environments using deep learning techniques.
2. To improve detection accuracy by leveraging the hierarchical learning capabilities of deep neural networks.
3. To address IoT-specific challenges such as device heterogeneity, scalability, and limited computational resources.
4. To explore optimal feature representation methods for distinguishing normal and malicious network behavior.
5. To ensure the proposed model is lightweight and resource-efficient for deployment on constrained IoT devices.
6. To evaluate the model's performance across multiple metrics, including accuracy, false positive rate, and latency.
7. To enable real-time intrusion detection through efficient inference and response mechanisms.
8. To generate actionable insights for proactive security management and policy enforcement in IoT networks.

2 Literature Survey

The rapid expansion of the Internet of Things (IoT) has introduced significant security challenges, spurring extensive research into intelligent Intrusion Detection Systems (IDS). Traditional rule-based IDS are increasingly inadequate, especially in detecting zero-day attacks or adapting to dynamic traffic patterns. Consequently, machine learning (ML) and deep learning (DL) approaches have gained prominence for developing adaptive IDS.

2.1 Machine Learning-Based Intrusion Detection Systems

ML techniques can learn from network traffic patterns to identify unknown threats. For example, a deep learning model evaluated on the BoT-IoT dataset [4] outperformed traditional ML methods but lacked scalability and suffered from high false positives in real-time use. Another framework [5] combined ML with Software Defined Networking (SDN) and Network

Function Virtualization (NFV) for a comprehensive solution yet raised concerns about overhead in resource-constrained IoT environments.

Feature selection significantly influences ML performance. A genetic algorithm-based method [12] enhanced Decision Tree and SVM classifiers but was computationally expensive and omitted dynamic features. A hybrid k-NN and Random Forest model [13] achieved high accuracy on multiple datasets but struggled with false positives in scenarios involving legitimate behavior variations.

Several studies proposed hybrid models to improve accuracy and reduce false alarms. An SVM-clustering approach [14] and a deep autoencoder model [15] showed promise but faced challenges such as complex tuning, long training times, and degraded performance under noisy, nonstationary data—conditions typical in real-world IoT environments.

Despite these efforts, most models:

- Use static or default features, ignoring feature redundancy and relevance.
- Rely on single-learning models, increasing risks of overfitting or high computational demand.
- Exhibit poor generalization across diverse datasets or deployment conditions.

These limitations underscore the need for IDS solutions that dynamically optimize features, are lightweight, and generalize well.

2.2 Comparative Analysis of Datasets

Datasets are foundational to evaluating IDS performance. While UNSW-NB15 is widely used for its realistic traffic and diverse attacks, older datasets like KDD Cup 1999 are outdated [2]. Other datasets, such as BoT-IoT and CICIDS2017, offer variations in protocol and class balance but present challenges in real-time applicability.

A recurring issue is poor generalization across datasets, often due to overfitting and imbalanced class distributions. This results in biased detection, particularly toward frequently occurring attack types. Many studies stress the importance of careful dataset selection and robust feature engineering for reliable IDS benchmarking.

2.3 Key Takeaways and Research Gaps

Identified gaps in current research include:

- Lack of Feature Optimization: Static feature sets reduce classifier effectiveness.
- Use of Single Models: Isolated use of CNN, SVM, or LSTM limits flexibility and robustness.
- Poor Generalization: Models often underperform on unseen data or in varied deployment environments.
- Neglect of Lightweight Design: Many deep models are too resource-intensive for constrained IoT devices.

2.4 Positioning of the Proposed Work

To address these gaps, we propose a hybrid IDS framework combining Particle Swarm Optimization (PSO) and Artificial Bee Colony (ABC) for feature selection, alongside a Deep Convolutional Neural Network (DCNN) for hierarchical feature extraction and classification. This approach aims to:

- Reduce redundant features and computational overhead,
- Improve generalization and prevent overfitting via swarm intelligence,
- Enhance real-time adaptability and efficiency in IoT environments.

Recent studies further validate the hybrid approach. Abdulkareem combined CNN, BiGRU, and BiLSTM with PSO, achieving 98.11% accuracy but requiring extensive tuning. Yaras and Dener achieved 99.96% accuracy using a CNN-LSTM model on CICIoT2023, though with high resource demands.

These findings reinforce the growing trend toward hybrid IDS models while highlighting the ongoing need for lightweight, scalable architectures—precisely what our PSO-ABC-DCNN model seeks to deliver.

2.5 Dataset And Feature Selection

One of the major challenges in developing effective IDS is the unavailability of comprehensive and realistic benchmark datasets that accurately reflect modern network traffic. The UNSW-NB15 dataset, created by the University of New South Wales (h ttps://research.unsw.edu.au/projects/unsw-nb15-dataset), addresses this gap by offering a hybrid dataset that includes both

real-world normal activities and synthesized attack scenarios. UNSW-NB15 dominates the defects of the BotIot dataset (for instance,no modern attacks, etc.) and has inchmeal become the most favorite dataset in the area of IoT intrusion detection in recent years. This dataset has become a crucial resource for evaluating IDS performance, particularly in IoT environments. Researchers have utilized machine learning techniques to analyze the features within this dataset, focusing on overcoming the "curse of high dimensionality" to enhance intrusion detection accuracy[1].

Table 1. UNSW-NB15 Data Set Statistics

Statistical features		16 hours	15 hours
No._of_flows		987,627	976,882
Src_bytes		4,860,168,866	5,940,523,728
Des_bytes		44,743,560,943	44,303,195,509
Src_Pkts		41,168,425	41,129,810
Dst_pkts		53,402,915	52,585,462
Protocol types	TCP	771,488	720,665
	UDP	301,528	688,616
	ICMP	150	374
	Other	150	374
Label	Normal	1,064,987	1,153,774
	Attack	22,215	299,068
Unique	Src_ip	40	41
	Dst_ip	44	45

The 9 types of attack categories are Analysis, Fuzzers, Exploits, Shellcode, Reconnaissance, DOS, Backdoors, Shellcode, and Worms of UNSW-NB15 Training Dataset and as represented by the graph in (Figure 1).

The bar chart in Figure 2 presents the category-wise statistics for the BOT-IoT dataset. The x-axis represents different categories of network traffic—Normal, DDOS, DoS, Reconnaissance, and Keylogging—while the y-axis shows the corresponding number of records. Among all categories, the Normal traffic has the highest count at 8,945, followed by DoS attacks with 6,391 records and DDOS attacks with 2,765 records. Reconnaissance and Keylogging have significantly lower frequencies, with 293 and 73 records, respectively. This distribution highlights a substantial imbalance in the dataset, with normal and DoS-related traffic dominating over other attack types.

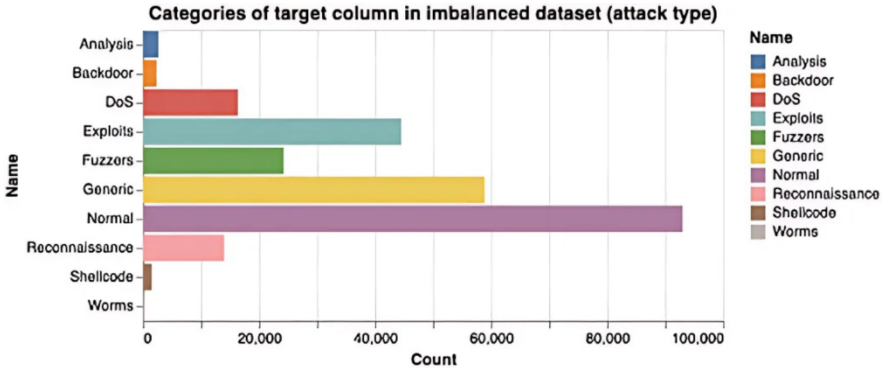

Fig 1. UNSW-NB15 Dataset Statistics

Figure 3 illustrates the dataset statistics for two widely used intrusion detection datasets—UNSW-NB15 and Bot-IoT—showing the number of records in the training and testing sets for each attack category.

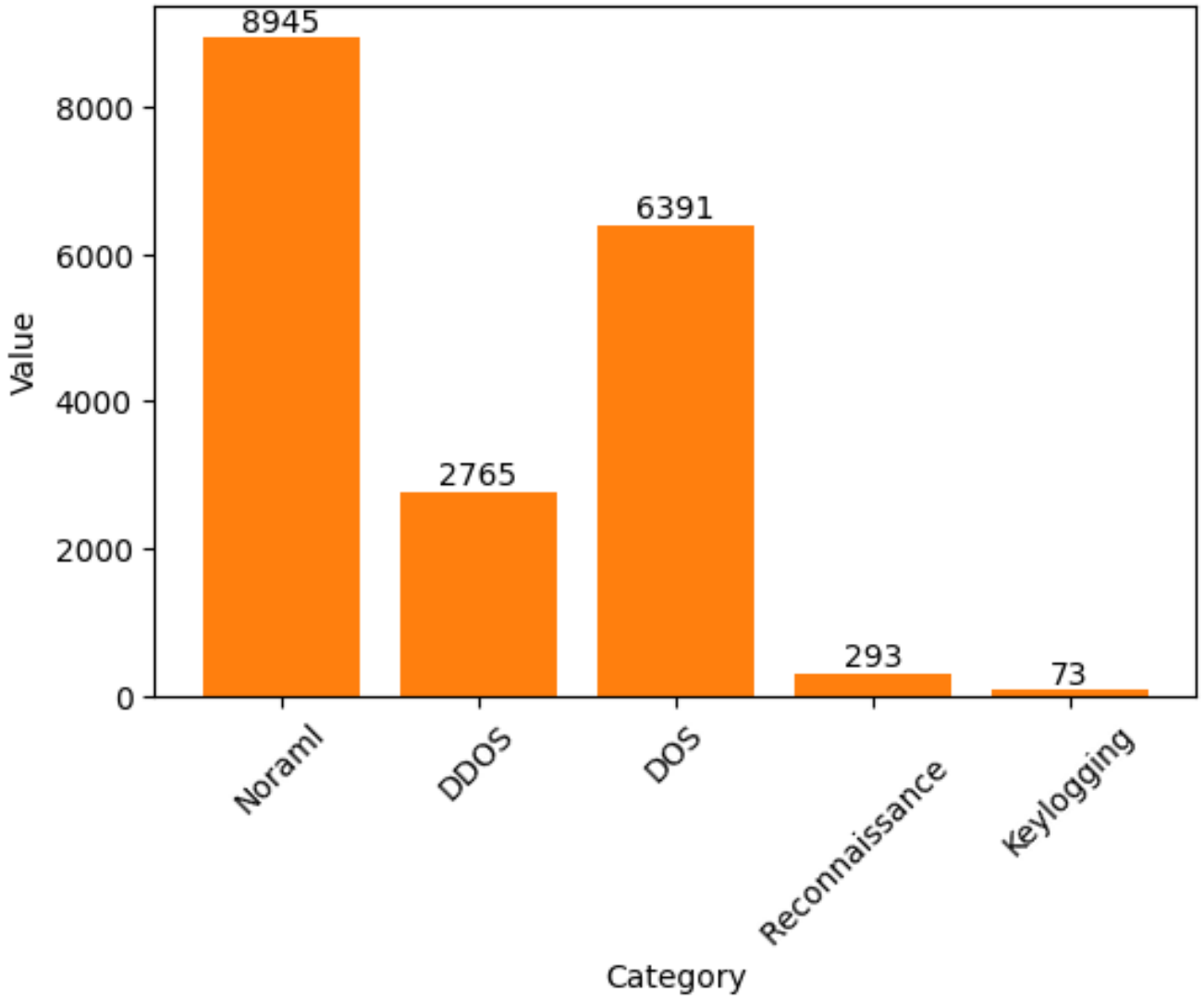

Fig 2. BOT-IOT Dataset Statistics

Dataset	Category	Training Dataset	Testing Dataset
UNSW-NB15	Normal	56,000	37,000
	Fuzzers	18,184	6062
	Analysis	2000	677
	Backdoors	1746	583
	DoS	12,264	4089
	Exploits	33,393	11,132
	Generic	40,000	18,871
	Recon.	10,491	3496
	Shell	1133	378
	Worms	130	44
	Total	175,341	82,332
Bot-IoT	Normal	286	191
	DoS	146,293	97,529
	DDos	163,287	108,858
	Recon.	54,649	36,433
	Theft	47	32
	Total	364,562	243,043

Fig 3. Dataset Statistics

For UNSW-NB15, the dataset includes multiple categories such as Normal (56,000 training, 37,000 testing), Fuzzers (18,184 training, 6,062 testing), Analysis (2,000 training, 677 testing), Backdoors (1,746 training, 583 testing), DoS (12,264 training, 4,089 testing), Exploits (33,393 training, 11,132 testing), Generic (40,000 training, 13,281 testing), Reconnaissance (10,491 training, 3,796 testing), Shellcode (1,133 training, 378 testing), and Worms (130 training, 44 testing). The total dataset contains 175,341 training records and 82,332 testing records.

For Bot-IoT, the categories include Normal (286 training, 191 testing), DoS (146,280 training, 101,888 testing), DDoS (163,287 training, 103,843 testing), and Reconnaissance (54,667 training, 36,453 testing).

This comparison shows that UNSW-NB15 has a more diverse set of attack types but with a relatively balanced distribution, while Bot-IoT contains fewer categories but a much larger volume of DoS and DDoS attack records, indicating class imbalance.

Feature selection plays a critical role in optimizing IDS performance. By employing techniques such as Information Gain (IG) and Gain Ratio (GR), researchers have been able to identify the most relevant features for detecting specific types of attacks, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.[3]. In[16] they have only top 4 features of the UNSW-NB15 Dataset that are extracted from the total 45 features by using the combination fusion algorithm of Random Forest algorithm and Decision tree classifier.

2.6 Proposed Method

This section elaborates on the proposed hybrid intrusion detection framework that integrates Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC), and Deep Convolutional Neural Networks (DCNN). The architecture addresses limitations such as high-dimensionality, poor feature representation, and overfitting, often encountered in IoT-based Intrusion Detection Systems (IDS).

2.6.1. Overview of the Proposed Framework

The proposed approach is designed as a three-phase system:

1. Deep Feature Extraction using DCNN
2. Feature Optimization using a hybrid PSO-ABC algorithm
3. Classification using a Multilayer Perceptron (MLP)

The core novelty lies in combining neighbourhood-based swarm intelligence with deep feature extraction to enhance both accuracy and generalizability in detecting IoT network intrusions.

2.6.2. Hybrid Optimization Algorithm

2.6.2.1. Particle Swarm Optimization (PSO):. PSO is a population-based metaheuristic inspired by the social behavior of birds and fish. In PSO, each candidate solution is represented by a particle, which adjusts its position and velocity in the search space based on both its own experience and that of neighboring particles.

The velocity and position update equations are given by:

$$v_i(t+1) = w \cdot v_i(t) + c_1 \cdot r_1 \cdot (pbest_1 - x_i(t)) + c_2 \cdot r_2 \cdot (gbest_1 - x_i(t)) \quad (1)$$

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad (2)$$

Where:

$v_i(t)$ is the velocity of particle i at time t,
$x_i(t)$ is the position of particle i,
$pbest_i$ is the personal best position of particle iii,
gbest is the global best position found by the swarm,
r_1 and r_2 are random values between 0 and 1,
w is the inertia weight, which controls the exploration vs. exploitation trade-off,
c_1 and c_2 are cognitive and social coefficients.

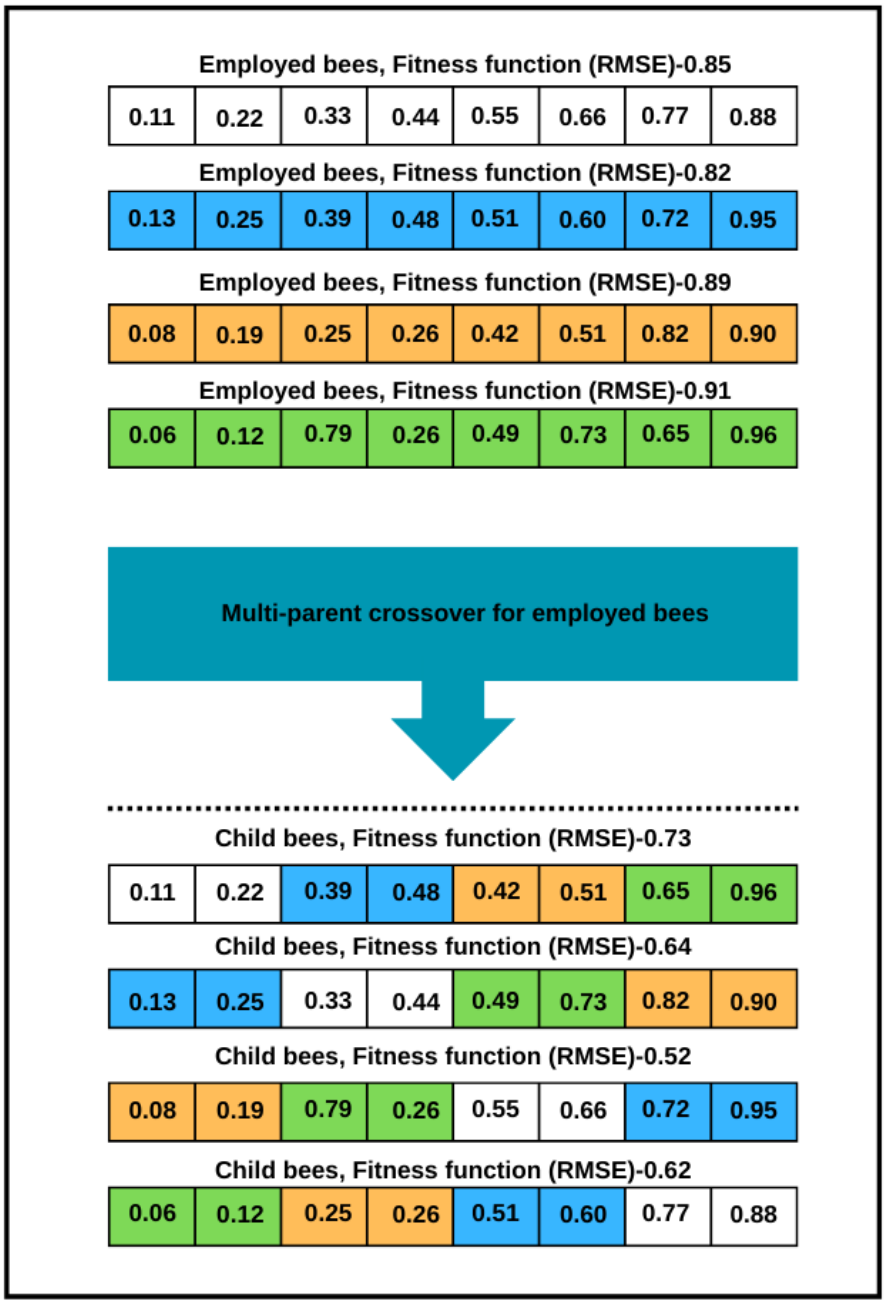

Fig 4. An example of a neighbourhood search around employed bees

2.6.2.2. Enhancement via Artificial Bee Colony (ABC):. To enhance exploration and avoid premature convergence, the PSO framework is augmented with Artificial Bee Colony (ABC) mechanisms:

- Employed Bees: Represent top-performing particles (global best regions)
- Onlooker Bees: Perform local neighborhood searches around employed bees
- Replacement Strategy: If an onlooker finds a better solution, it replaces its corresponding employed bee

This hybridization introduces dynamic neighbourhood search capabilities, improving both convergence speed and solution diversity.

2.6.2.3. Multi-Parent Crossover:. Standard PSO can suffer from diminishing diversity as particles converge. To address this, a multi-parent crossover mechanism is introduced:

- All employed bees participate in generating new solutions.
- Offspring solutions are created by combining attributes from multiple parent particles.
- This ensures diverse and widely-explored search spaces, reducing the risk of local optima entrapment.

2.7 Deep Feature Extraction with DCNN

DCNN is employed to extract hierarchical, high-level features from the UNSW-NB15 dataset. The architecture includes:

- Input Layer: Raw feature vector from network traffic
- Convolutional Layers: Detect spatial features and local patterns
- Pooling Layers: Downsample feature maps, reduce dimensionality
- Fully Connected Layers (MLP)**:** Classify optimized feature vectors

DCNN learns relevant representations without requiring manual feature engineering, and the extracted features are fed into the PSO-ABC optimizer.

2.8 Workflow of the Proposed System

The integration of DCNN with the PSO-ABC optimization strategy proceeds as follows:

1. Preprocessing: Normalize and encode features from the UNSW-NB15 dataset.
2. DCNN Feature Extraction: Apply convolutional and pooling layers to obtain deep features.
3. Optimization:
    - Initialize PSO particles using deep features.
    - Apply ABC-enhanced PSO search for optimal feature subset and hyperparameters.
    - Employ multi-parent crossover to ensure diverse solution search.
4. Classification: Use optimized features to train an MLP classifier.
5. Evaluation: Assess performance using standard metrics.

This algorithm enhances the traditional PSO by incorporating the neighborhood search and update mechanisms from the ABC algorithm, resulting in a more robust and effective optimization process. This hybrid approach leverages the strengths of both PSO and ABC, making it well-suited for complex optimization problems where the search space is large and the risk of local minima is significant.

Feature Extraction: A Deep Convolutional Neural Network (DCNN) is employed to extract high-level features from the input data. These features are then used to represent the particles in the PSO algorithm, providing a more informed and structured search space.

Particle Representation: The particles in the PSO algorithm are not just simple vectors but are represented by the deep features extracted by the DCNN, which encapsulates the most relevant information from the data.

Enhanced Search: By using deep features, the algorithm can perform more sophisticated searches, leveraging the hierarchical representation of data to navigate complex solution landscapes effectively.

The algorithm iteratively repeats the process of neighborhood search, updating employed bees, refining the global best, and enhancing the feature representation through the DCNN until a termination condition is met. The overall schematic of the

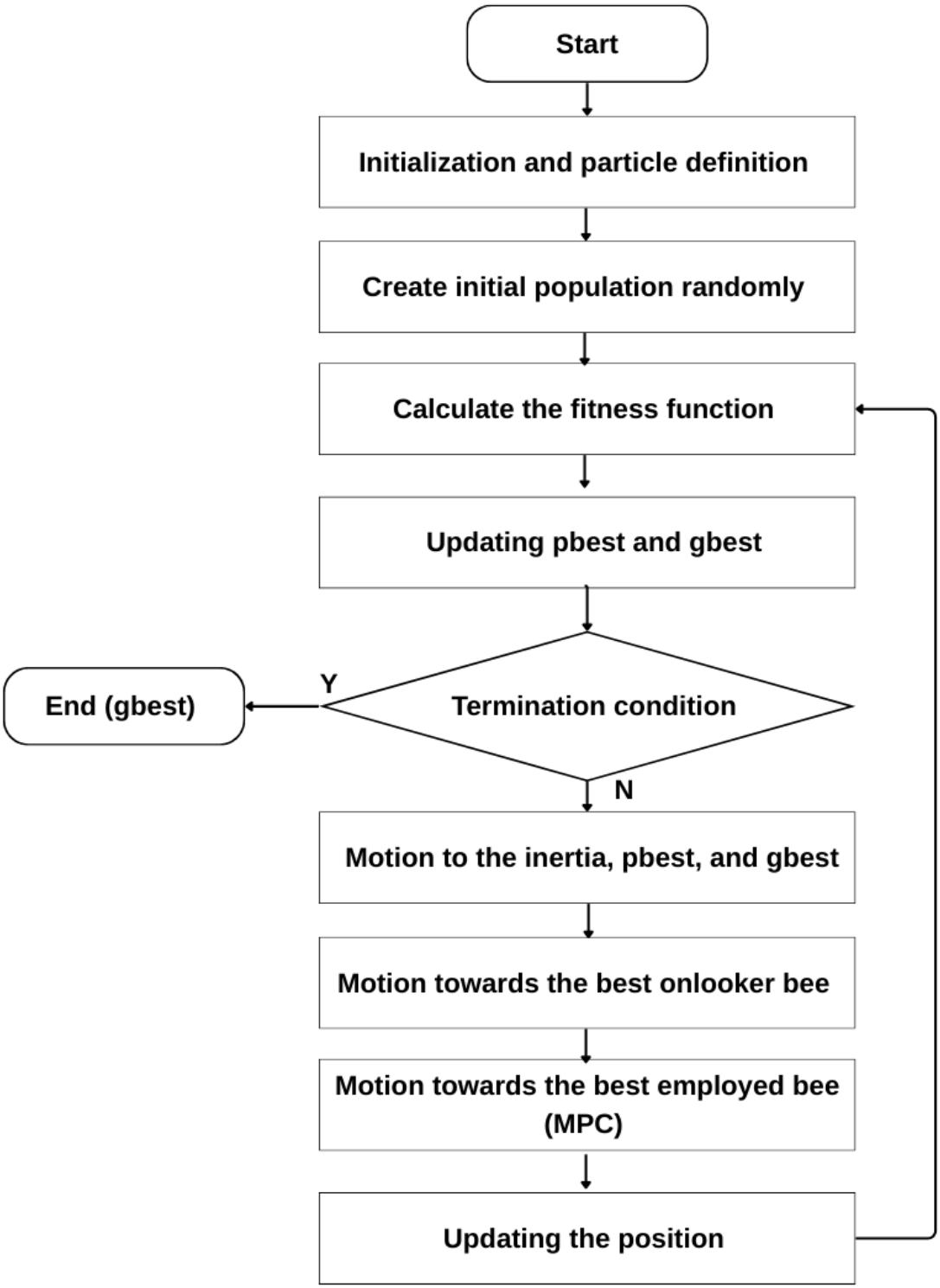

Fig 5. Flowchart of ABC algorithm

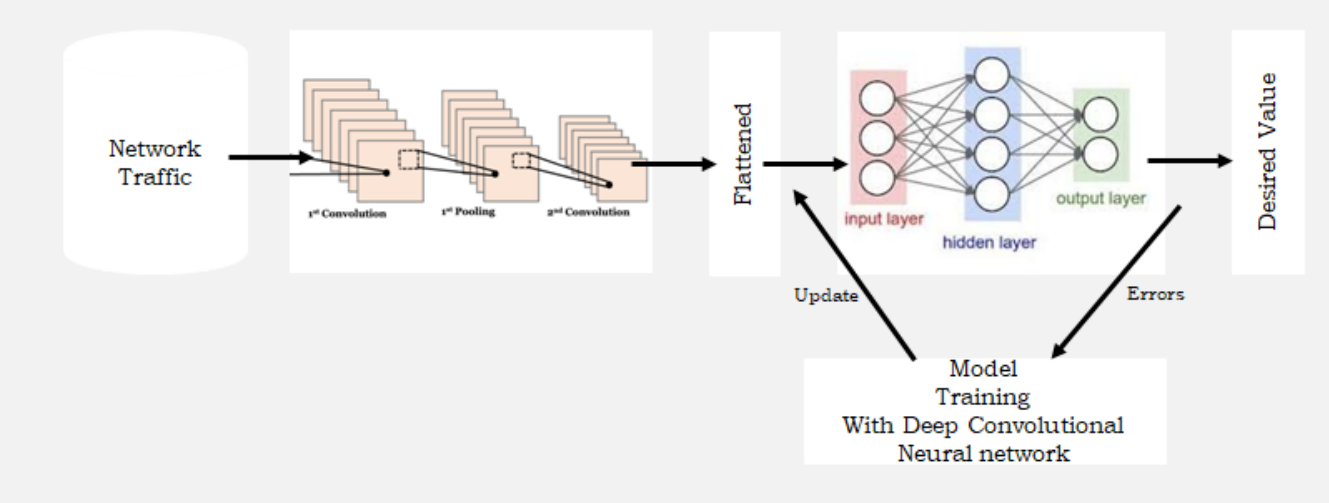

Fig 6. Overall Flow Chart of deep learning algorithm

proposed classifier is depicted in Figure 5. According to this figure, the input data passes through some convolution and pooling layers. After that, we use a fully connected MLP to classify the datasets. The fully connected MLP is trained by the proposed in order to achieve a higher classification and detection rate. Figure 6 shows the flowchart of the deep learning algorithm.

$$\text{Mean Square Error (MSE)} = \frac{1}{k}\sum_{i=1}^{k}(O_i - D_i)^2 \tag{3}$$

where, k = the total number of samples, Oi = system output, and Di = desire.

For validation, accuracy metrics are used to compare the performance of the deep architectures.

2.8.1. Experimental Setup:

- Dataset: UNSW-NB15, including 10 attack categories and normal traffic
- Split: 70% training, 30% testing
- Development Tools: Python, TensorFlow, Keras, Scikit-learn
- Baseline Models**:** Compared against SVM, CNN, LSTM, RNN

Hyperparameters:

- PSO: Population = 30, ,
- ABC: Onlooker bees = 30, Limit = 5 (abandonment threshold)

This configuration enables comprehensive evaluation of the proposed system's adaptability and accuracy across varied IoT threat patterns.

This hybrid model demonstrates a powerful combination of evolutionary optimization and deep learning to address the limitations of traditional IDS frameworks in IoT environments.

3 Results and Discussion

Intrusion detection in Internet of Things (IoT) environments presents unique challenges due to the scale, heterogeneity, and real-time nature of device communications. Traditional machine learning approaches often suffer from limited adaptability, high feature complexity, and poor generalization across diverse attack types. To address these concerns, this study introduces a novel hybrid algorithm that integrates Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC), and Deep Convolutional Neural Networks (DCNN).

3.1 Performance Overview

The proposed model was evaluated using the UNSW-NB15 dataset. It achieved a detection accuracy of 99.41%, outperforming several benchmark algorithms across a range of IDS studies. This result underscores the effectiveness of combining deep learning with swarm intelligence for handling high-dimensional and complex IoT traffic data.

By utilizing DCNN for automatic hierarchical feature extraction and optimizing the input features using PSO enhanced with ABC's neighborhood search, the model demonstrates robust generalization, reduced false positives, and improved detection sensitivity.

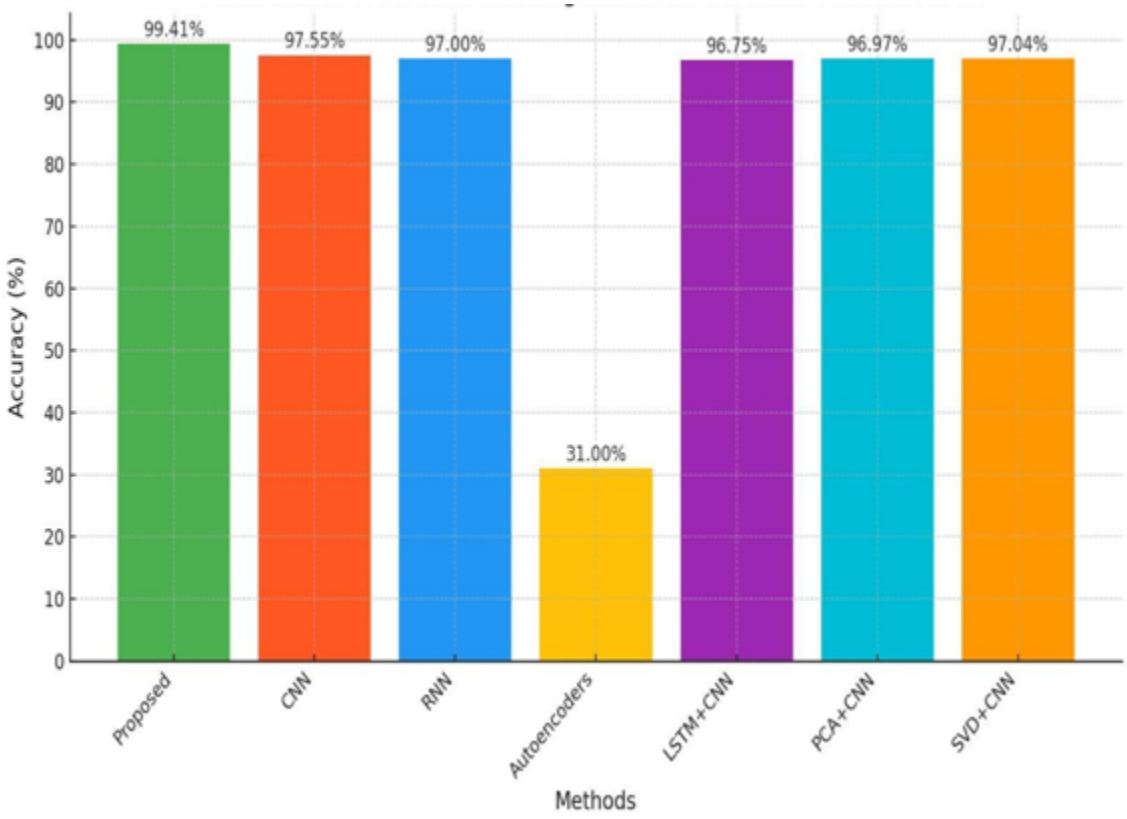

Fig 7. Accuracy bar chart of deep learning algorithms

To validate the effectiveness of the proposed method, it was compared with a range of classical and modern algorithms from the literature, as shown in Table 2.

Table 2. Analysis with accuracy of various algorithms

References	Algorithm	Accuracy	Dataset
(7)	SVM on KDD	99.24	KDD
(17)	SDN	90%	Bot IOT
(18)	RNN	98.27	UNSW-NB 15
(19)	Neural Network LSTM	99.03%	CISIDS 2017
(20)	ANN	84%	UNSW-15
(21)	CNN	92.85%	Bot IOT
-	Proposed Algorithm	99.41	UNSW-NB 15

The proposed model achieves the highest accuracy among all models compared, particularly excelling on the UNSW-NB15 dataset. This illustrates its capacity to generalize across complex traffic types and its suitability for deployment in real-world IoT environments.

3.2 Discussion

The results reveal multiple advantages of the proposed hybrid system:

- Robust Feature Selection: By employing PSO with ABC's neighborhood search, the system reduces the impact of noisy and redundant features.
- Improved Generalization: The DCNN structure enables learning complex attack signatures, even from imbalanced and high-dimensional input data.
- Diversity in Optimization: The use of multi-parent crossover promotes global exploration and avoids premature convergence—common in standard PSO or GA-based models.

In contrast to traditional IDS models, which often require manual tuning and extensive feature engineering, this approach is fully automated and scalable.

3.3 Real-World Implications

The model's lightweight nature and high detection precision make it an ideal candidate for real-time IDS in resource-constrained IoT devices. Its adaptability also suggests strong potential for deployment in smart homes, industrial IoT networks, and smart city infrastructure where security and scalability are crucial.

In summary, the proposed model not only achieves superior detection performance but also addresses the core limitations of traditional machine learning-based IDS systems. It sets a new benchmark for future research in intelligent intrusion detection in IoT contexts.

4 Conclusion

The evolving landscape of IoT security necessitates intelligent, adaptive, and lightweight Intrusion Detection Systems (IDS). While numerous machine learning and deep learning-based approaches have demonstrated effectiveness, they often suffer from limitations such as high false positive rates, poor generalization, and computational inefficiency in real-time or resource-constrained environments. A key observation is the underutilization of dynamic feature optimization and the overreliance on single-model architectures.

This work addresses these challenges by proposing a hybrid IDS framework that combines metaheuristic optimization (PSO and ABC) for efficient feature selection with a Deep Convolutional Neural Network (DCNN) for robust classification. This integrated approach aims to enhance detection accuracy, reduce computational overhead, and improve adaptability across diverse IoT environments.

Recent research further supports the efficacy of hybrid models, though many still face deployment challenges due to model complexity. Our proposed PSO-ABC-DCNN framework advances the state of the art by focusing on both performance and scalability, making it a promising candidate for real-world IoT intrusion detection applications.

References

1) Venkatachalam K, Jacob P. UNSW-NB15 Dataset Feature Selection and Network Intrusion Detection Using Deep Learning. *International Journal of Recent Technology and Engineering (IJRTE)*. 2019;7(6):63–67. Available from: https://www.researchgate.net/publication/332265020_UNSW-NB15_dataset_feature_selection_and_network_intrusion_detection_using_deep_learning.
2) Diro M, Chilamkurti N. Leveraging LSTM and GRU for Network Intrusion Detection Using UNSW-NB15 Dataset. *ICT Express*. 2020;6(4):312–319. https://doi.org/10.1016/j.icte.2020.07.002.
3) Chen MS, Xu HH, Zheng XX. Feature Selection for Intrusion Detection Systems in IoT. 2021. https://doi.org/10.1186/s40537-024-00892-y.
4) Zamani AK, Chapnevis A. BotNet Intrusion Detection System in Internet of Things with Developed Deep Learning. *arXiv preprint arXiv:220704503*. 2022.
5) Tahsien SM, Karimipour H, Spachos P. Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey. *arXiv preprint arXiv:200405289*. 2020. Available from: https://arxiv.org/abs/2004.05289.
6) Hussain F, Hussain R, Hassan SA, Hossain E. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials*. 2020;22(3):1686–1721. https://doi.org/10.1109/COMST.2020.2986444.
7) Bagaa M, Taleb T, Bernabe JB, Skarmeta AJ. A Machine Learning Security Framework for Internet of Things Systems. *IEEE Access*. 2020;8:42573–42585. https://doi.org/10.1109/ACCESS.2020.2976794.
8) Gueriani A, Kheddar H, Mazari AC. Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems. *arXiv preprint arXiv:240518624*. 2024.
9) Khairullah EF, Alsenani N. A Comprehensive Study of Deep Learning Models for Intrusion Detection in IoT Devices. *Engineering, Technology & Applied Science Research*. 2025;15(2):21029–21036. https://doi.org/10.48084/etasr.9490.
10) Abdulkareem AB. Advances in IoT Intrusion Detection: Deploying Hybrid Deep Learning and Metaheuristic Algorithms for Optimal Feature Selection. *Ingénierie des systèmes d information*. 2025;30(4):1027–1041. http://dx.doi.org/10.18280/isi.300419.

11) Yaras S, Dener M. IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm. *Electronics*. 2024;13(6):1053. https://doi.org/10.3390/electronics13061053.
12) Gupta A, et al. A novel feature selection and classification approach for IoT intrusion detection. *IEEE Access*. 2021;9:34656–34668. https://doi.org/10.1109/ACCESS.2021.3064732.
13) Ahmed M, Mahmood AN, Hu J. A survey of network anomaly detection systems using machine learning techniques. *Journal of Network and Computer Applications*. 2020;151:102492. https://doi.org/10.1016/j.jnca.2019.102492.
14) Khan MA, et al. A hybrid machine learning model for intrusion detection in IoT networks. *Journal of Ambient Intelligence and Humanized Computing*. 2021;12(3):3075–3086. https://doi.org/10.1007/s12652-020-02355-2.
15) Shatnawi AM, et al. Deep learning-based anomaly detection for IoT systems using autoencoders. *IEEE Transactions on Network and Service Management*. 2022;19(2):1155–1167. https://doi.org/10.1109/TNSM.2022.3154237.
16) Kanimozhi V, Jacob P. UNSW-NB15 Dataset Feature Selection and Network Intrusion Detection using Deep Learning. *International Journal of Recent Technology and Engineering*. 2019;7(5S2). Available from: https://www.ijrte.org/download/volume-7-issue-5s2/.
17) Karie NM, Sahri NM, Haskell-Dowland P. A Survey on Security Threats and Detection Methods in Internet of Things. *IEEE Access*. 2020;8:174962–174989. https://doi.org/10.1109/ACCESS.2020.3026981.
18) Sivanathan A, Gharakheili HH, Sivarama V. Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning. *IEEE Transactions On Network And Service Management*. 2020;17(1). https://doi.org/10.1109/TNSM.2020.2968054.
19) Guerra-Manzanares A, Medina-Galindo J, Bahsi H, Nõmm S. MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network. *International Conference on Information Systems Security and Privacy (ICISSP)*. 2020;p. 207–218. http://dx.doi.org/10.5220/0009187802070218.
20) Roopak M, Tian GY, Chambers J. An intrusion detection system against DDoS attacks in IoT networks. *10th Annual Computing and Communication Workshop and Conference (CCWC)*. 2020;p. 562–567. https://doi.org/10.1109/CCWC47524.2020.9031206.
21) Hanif S, Ilyas T, Zeeshan M. Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset. *IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT)*. 2019;p. 152–156. https://doi.org/10.1109/HONET.2019.8908122.