Indonesian Journal of Electrical Engineering and Computer Science
Vol. 40, No. 2, November 2025, pp. 1040~1049
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v40.i2.pp1040-1049

Enhancing IoT security: a hybrid intelligent intrusion detection system integrating machine learning and metaheuristic algorithm

Sanaa A. A. Ghaleb[1,2,3], Mumtazimah Mohamad[1,4], Waheed Ghanem[3,5,6], Amir Ngah[5], Farizah Yunus[5], Arifah Che Alhadi[5], MD Nurul Islam Siddique[7]
[1]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin (UniSZA), Terengganu, Malaysia
[2]Faculty of Education, University of Aden, Aden, Yemen
[3]Faculty of Engineering, University of Aden, Aden, Yemen
[4]Artificial Intelligence for Sustainability and Islamic Research Center, Universiti Sultan Zainal Abidin, Terengganu, Malaysia
[5]Faculty of Computer Science and Mathematics, Universiti Malaysia Terengganu (UMT), Terengganu, Malaysia
[6]Faculty of Education, University of Lahej, Lahej, Yemen
[7]Faculty of Ocean Engineering Technology, Universiti Malaysia Terengganu, Terengganu, Malaysia

Article Info

Article history:

Received Sep 18, 2024
Revised Aug 3, 2025
Accepted Oct 15, 2025

Keywords:

Classification
Internet of things
Intrusion detection system
Moth search algorithm
Multilayer perceptron

ABSTRACT

The rapid proliferation of the internet of things (IoT) has introduced significant security and privacy challenges. As IoT devices often have limited computational power and memory, they are highly vulnerable to cyber threats. Traditional intrusion detection systems (IDS) struggle to operate efficiently in these constrained environments, necessitating more adaptive and optimized security solutions. To address these challenges, this study proposes an innovative IDS model, MSAMLP, which combines the moth search algorithm (MSA) with a multilayer perceptron (MLP) classifier. The objective is to enhance the classification accuracy of malicious and benign network traffic while maintaining computational efficiency. The model was evaluated using two widely recognized intrusion detection datasets, benchmarking its performance against existing IDS approaches. Experimental results indicate that MSAMLP outperforms conventional classification models, achieving high accuracy, improved detection rates, and reduced false alarm rates. Its adaptive learning capability ensures better anomaly detection in dynamic IoT environments. In conclusion, the proposed MSAMLP model demonstrates superior performance in securing IoT networks, offering an effective solution to mitigate evolving cyber threats. This research contributes to the advancement of IoT security by introducing a robust and scalable intrusion detection approach.

Corresponding Author:

Mumtazimah Mohamad
Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin (UinSZA)
Besut, Terengganu, Malaysia
Email: mumtaz@unisza.edu.my

1. INTRODUCTION

The internet of things (IoT) despite its potential benefits, also brings several significant challenges. The merging of "internet" and "things" into a single framework can lead to substantial security vulnerabilities, as millions of interconnected devices become potential targets for cyberattacks [1], [2]. The reliance on the standard internet protocol suite (TCP/IP) means that any weakness in this foundational technology can have widespread implications [3], [4]. Moreover, the proliferation of IoT devices raises

concerns about data privacy, as vast amounts of personal and sensitive information are collected, often without explicit consent [5]. The integration of private, public, commercial, and governmental networks increases the complexity of managing and securing these systems, making it difficult to protect against unauthorized access and data breaches [6]. Thus, while the IoT aims to create a seamless network of networks, it also presents a host of risks that must be carefully addressed to ensure its safe and ethical deployment [7]. While previous studies have explored IoT security from different perspectives, they have not sufficiently addressed the impact of network protocol vulnerabilities on data security in IoT environments [8]. Furthermore, much of the existing research has focused on traditional security solutions such as firewalls and encryption, without providing effective mechanisms for detecting sophisticated cyber threats using artificial intelligence and behavioral analysis [9]. Therefore, this study aims to explore advanced strategies and developments for strengthening intrusion detection systems (IDS) in IoT environments by leveraging cutting-edge methodologies such as machine learning, anomaly detection, and behavior analysis. By utilizing these techniques, organizations can enhance their defenses against evolving cyber threats, ensuring the security and privacy of IoT ecosystems [10].

2. RELATED WORK

In recent years, numerous studies have been proposed to improve the classification accuracy of malicious and benign network traffic. Yin *et al.* [11], proposed information gain and random forest-recursive feature elimination (IGRF-RFE), a hybrid feature selection method designed to improve multi-class network anomaly detection using a multilayer perceptron (MLP) network. This method combines filter techniques (information gain and random forest) in the initial phase to address less relevant features effectively. In the next phase, a machine learning (ML)-based wrapper technique, recursive feature elimination, is employed to further reduce the feature dimensions while considering the relevance of similar feature. The findings from the UNSW-NB15 dataset show that the proposed method enhances anomaly detection by reducing the number of features from 42 to 23, resulting in an accuracy increase 84.24%. Sayegh *et al.* [12], presented an advanced IDS specifically designed for IoT networks. To address the challenge of imbalanced data in IDS development, the study incorporates synthetic minority over-sampling technique (SMOTE). This technique helps the system accurately identify rare intrusion patterns by generating synthetic instances for the minority class. Unlike other methods, such as generative adversarial networks (GANs), the study evaluates the IDS using the NSL-KDD dataset and demonstrates that the long short-term memory (LSTM)-based IDS, combined with SMOTE to handle data imbalance, surpasses existing techniques in precisely detecting IDs. Rabie *et al.* [13] introduced a new framework that combines decisive red fox (DRF) with descriptive back propagated radial basis function (DBRF) classification. This integration marks a significant advancement by merging the state-of-the-art DRF optimization approach with ML techniques to enhance security in IoT systems. The proposed framework covers essential phases like data preprocessing, normalization, and the use of EFO optimization to tailor features specifically for IDs. The authors utilized logistic regression (LR), decision tree (DT), and random forest (RF) algorithms for the classification stage. Karthikeyan *et al.* [14], proposed a novel firefly algorithm-based machine learning (FA-ML) approach for intrusion detection, leveraging a support vector machine (SVM) classifier optimized using the grey wolf optimizer (GWO). Experimental evaluations on the NSL-KDD dataset demonstrated that the K-nearest neighbor-particle swarm optimization (KNN-PSO) technique achieved a remarkable accuracy of 96.42%, outperforming extreme gradient boosting (XGBoost) (95.36%). Finally, Good *et al.* [15] conducted a comparative study on IoT anomaly detection models using the NSL-KDD dataset. They applied ML algorithms, including XGBoost, SVM, and deep convolutional neural network (DCNN), to classify anomalies in network traffic. The research was conducted using the NSL-KDD dataset. Furthermore, a noteworthy contribution emerged with the development of a novel IDS model, leveraging the promising moth search algorithm (MSA). This model effectively overcame challenges associated with conventional MLP training techniques, achieving enhanced accuracy in identifying IDSs within IoT environments. These achievements were validated across the IDS benchmark dataset.

3. PROPOSED METHOD

The MSAMLP-IDS model, as illustrated in Figure 1, aims to implement an intrusion detection (ID) approach using artificial neural networks (ANNs) trained through the MSA. The primary objective is to achieve high detection accuracy, reduce false positives, improve convergence speed, and effectively identify security events (SE). This is accomplished by utilizing MSA as a metaheuristic optimization algorithm to train ANNs within the proposed framework. Multilayer perceptron neural networks (MLPNN) are powerful classification tools known for their ability to analyze security data in IoT environments and detect anomalies based on statistical significance. These networks feature a flexible and scalable architecture, enabling them to

develop a comprehensive model of environmental behavior and pattern recognition. The proposed model consists of three main modules, as illustrated in Figure 1. The IDS dataset module is responsible for data management, filtering, and feature extraction, ensuring that relevant and high-quality data is processed for model training.

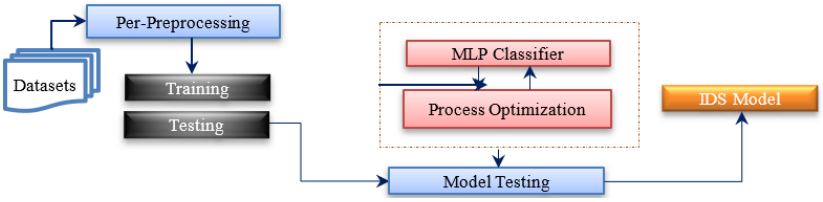


Figure 1. The MSAMLP-IDS model

The neural network module (NN module) consists of a MLPNN structured with an input layer, multiple hidden layers, and an output layer, allowing for efficient learning and classification. To enhance model performance, the optimization module employs the MSA to fine-tune the neural network's structure and weights, optimizing its accuracy and adaptability in detecting intrusions effectively. The Figure 1 illustrates the key stages of executing the MSAMLP-IDS model for intrusion detection, from data input to final model evaluation. The process begins with system initialization and loading of IDS data. Data processing follows, including data cleaning to remove incorrect or missing values, data normalization to scale numerical values within a specific range [-1, +1] for consistency and enhanced model performance, and data splitting to divide the dataset into training and testing sets. This ensures that the model is trained on one portion of the data and evaluated on another for accurate performance assessment. After data preparation, a MLPNN is constructed, consisting of input, hidden, and output layers, with the number of neurons in each layer determined based on predefined parameters [16], [17]. During the training process, moth positions are initialized in the solution space, and the performance of each weight set is evaluated using mean squared error (MSE). The MSA then optimizes the neural network weights based on Lévy flights and straight-line movement toward the light source. The process stops once the maximum iterations are reached or when no further performance improvement is observed. After training, the model is tested using the test dataset, with performance evaluated through accuracy, recall, F1-score, and MSE. Future improvements could focus on incorporating real-time anomaly detection mechanisms, developing adaptive learning techniques, and implementing feature selection strategies to optimize model performance and reduce computational complexity, making IDS solutions more effective for real-world applications.

3.1. Moth search algorithm

The proposed algorithm plays a crucial role in enhancing intrusion detection by optimizing feature selection and improving classification accuracy. It integrates advanced techniques to ensure efficient processing and precise anomaly detection within IoT networks. Through rigorous evaluation and benchmarking against existing methods, the algorithm demonstrates superior performance in terms of accuracy, detection rate, and computational efficiency. Interested readers can refer to [18] for more in-depth details on the algorithm.

3.1.1. Lévy flights

The MSA algorithm employs Lévy flights to enhance search space exploration, where moth positions are updated using:

$$x_i^{t+1} = x_i^t + \alpha L(s)$$

where L(s) follows the Lévy distribution: L (s) ~ $|s|^{-B}$ where $1 < \beta \leq 3$.

3.1.2. Straight-line flight towards the target

When moths are far from a light source, they move directly toward it using:

$$x_i^{t+1} = \lambda \times (x_i^t + \phi \times (x_{best}^t - x_i^t))$$

where ϕ is a gradient factor inspired by the golden ratio, and λ is a random scaling factor.

3.2. Training algorithm

The proposed algorithm enhances intrusion detection by optimizing feature selection and improving classification accuracy through a structured training process. It begins with moth initialization, where initial values for weights and parameters are assigned. Next, the objective function computation (fitness function) is performed by calculating the MSE, defined as $\text{MSE} = \sum_{k=1}^{q} \frac{E_k}{q}$ where q is the number of training samples, and E_k is the error for each sample. Following this, weight updating via MSA takes place, optimizing weights and parameters iteratively to minimize the MSE. The stopping condition is met once convergence is achieved or the maximum iterations are reached. Through this approach, the algorithm ensures efficient processing and precise anomaly detection within IoT networks. Interested readers can refer to [19]–[22] for more in-depth details.

4. PERFORMANCE EVALUATION AND DISCUSSION

To ensure reproducibility, the experimental setup consists of an Intel Core i7 processor with 16 GB RAM, utilizing MATLAB R2024a for ANN implementation. The study employs two benchmark datasets: NSL-KDD, which contains 41 features categorized into attack types and normal connections [23], [24], and UNSW-NB15, which includes 9 modern attack types, normal activities, and 44 features plus a class label [25], as detailed in Table 1. The evaluation metrics used to assess model performance include accuracy, precision, recall, F1-score, and MSE. The proposed algorithm plays a crucial role in enhancing intrusion detection by optimizing feature selection and improving classification accuracy. Through rigorous evaluation and benchmarking against existing methods, the algorithm demonstrates superior performance in terms of accuracy, detection rate, and computational efficiency. Interested readers can refer to [22] for more in-depth details on the algorithm. To ensure reproducibility, the following experimental setup is used.

The dataset preprocessing in this study consists of two stages. First, a subset of records is randomly sampled from the large datasets, then split into training and testing sets. Second, categorical attributes are converted into numerical values, followed by normalization to ensure uniform processing. The NSL-KDD and UNSW-NB15 datasets are labeled for binary classification, distinguishing normal (0) from attack traffic (1). The parameters used for performance evaluation are detailed in Table 2. The partitioning description are displays in Table 3.

Table 1. Partitioning description of the dataset

Dataset	Train records	Test records
NSL-KDD	25,192	22,544
UNSW-NB15	175,341	82,332

Table 2. Partitioning description of the dataset

Algorithm	Parameter	Value
HS	Harmony memory size	50
	Harmony memory consideration rate	0.95
	Pitch adjustment rate	0.1
PBIL	Habitat modification probability	1
	Immigration probability	[0, 1]
	Step size for numerical integration	1
	Maximum immigration	1
	Mutation probability	0.005
SCA	Random number	[0, 1]
	Linear decreased	2
MFO	MFO linearly decreased	-1 to -2
	Logarithmic spiral	2
	Random number	[-1, 1]
PSO	Inertial constant	0.3
	Cognitive constant	1
	Social constant for swarm interaction	1
DE	Weighting factor	0.5
	Crossover constant	0.5
ABC	Limit	100
ES	λ	10, 1
	σ	50 for XOR and Balloon,
	Population size	200 for the rest /250
	Maximum number of generation	

Table 3. Partitioning description

Measure	Definition	Equation
Accuracy (ACC)	$((TP+TN)/(TP+TN+FP+FN))$	(1)
False alarm rate (FAR)	$(FP/(FP+TN))$	(2)
Specificity (SP)	$(TN/(TN+FP))$	(3)
F-measure (F1)	$((2\times PPV\times SN)/(PPV+SN))$	(4)
Detection rate (DR)	$(TP/(TP+FN))$	(5)
Sensitivity (SN)	$(TP/(TP+FN))$	(6)
G-mean (GM)	$\sqrt{(SN\times SP)}$	(7)
Matthews correlation coefficient (MCC)	$\sqrt{(TP+FP)(TP+FN)}((TP\times TN-FP\times FN)/(TN+FP)(TN+FN))$	(8)

5. RESULTS AND DISCUSSION

This study employs two conventional datasets to assess performance across different domains. To guarantee that the data is appropriately prepared for training MLPs, the min-max normalization technique was applied. This method standardizes feature values by rescaling them to a specified range, typically between 0 and 1. This normalization step ensures that all features contribute equally to the training process and improves the efficiency and effectiveness of the MLPs. The results derived from applying this approach to the datasets are detailed below, providing insights into how the performance of the MLPs varies across different scenarios and conditions.

5.1. Scenario 1: performance of the NSL-KDD dataset

The outcomes of the MSAMLP IDS method and its associated models are calculated utilizing (1)–(8) as outlined in Table 3. Table 4 offers an overview of the results for the MSAMLP IDS approach. In terms of accuracy, the MSAMLP algorithm demonstrates the highest performance, whereas POSMLP and DEMLP yield relatively similar lower percentages. The POSMLP algorithm produced results that were alike to MSAMLP, with an ACC of 97.81%, FAR of 0.0107, and DR of 96.96%. Following closely, the DEMLP ranked fourth in DR but third in both ACC and FAR, with percentages of 96.16%, 96.62%, and 0.0276, respectively. Meanwhile, the MFOMLP ranked third in DR but fourth in both ACC and FAR, with percentages of 96.24%, 96.61%, and 0.0289, respectively. Moving on, the PBILMLP algorithm secured the fifth position in both ACC and DR, while ranking eighth in FAR, attaining rates of 95.71%, 96.10%, and 0.0482, respectively.

Table 4. Performance classification across 9 algorithms in the NSL-KDD data set

Algorithms	Accuracy	DR	FAR	MCC	Sensitivity	Specificity	F1	G mean
ABC	93.79	92.21	0.0412	0.88	0.92	0.96	0.94	94.03
MSA	98.32	97.48	0.0057	0.97	0.97	0.99	0.99	98.45
DE	96.62	96.16	0.0276	0.93	0.96	0.97	0.97	96.70
ES	92.18	91.54	0.0697	0.84	0.92	0.93	0.93	92.28
HS	91.11	87.88	0.0462	0.83	0.88	0.95	0.92	91.55
MFO	96.61	96.24	0.0289	0.93	0.96	0.97	0.97	96.67
PBIL	95.71	96.10	0.0482	0.91	0.96	0.95	0.96	95.64
PSO	97.81	96.96	0.0107	0.96	0.97	0.99	0.98	97.94
SCA	94.52	92.73	0.0311	0.89	0.93	0.97	0.95	94.79

SCAMLP followed with a sixth position in both ACC and DR, and fifth in FAR, recording rates of 94.52%, 92.73%, and 0.0311, respectively. ABCMLP attained the seventh position in both ACC and DR, while ranking sixth in FAR, with rates of 93.79%, 92.21%, and 0.0412, respectively. Further down the list, the ESMLP algorithm secured the eighth position in both ACC and DR, and ninth in FAR, with rates of 92.18%, 91.54%, and 0.0697, respectively. Lastly, the HSMLP algorithm ranked ninth in both ACC and DR, and seventh in FAR, achieving rates of 91.11%, 87.88%, and 0.0462, respectively. Figure 2 illustrates the comparative performance of MSAMLP and other algorithms when tested on the NSL-KDD dataset. The analysis highlights the convergence speed of the MSE during training, demonstrating that MSAMLP outperforms other models in terms of rapid convergence, reinforcing the effectiveness of the proposed approach.

5.2. Scenario 2: performance of the UNSW-NB15 dataset

Table 5 and Figure 3 summarize the performance of the MSAMLP intrusion detection approach on the UNSW-NB15 dataset. The proposed approach achieves outstanding results, with an accuracy of 98.93%, a detection rate of 98.21%, and a false alarm rate of 0.0074. Other models were evaluated for comparison:

DEMLP ranked second in accuracy (97.83%) and DR (96.43%) but fifth in FAR (0.0151). SCAMLP secured second place in FAR (0.0106), third in accuracy (97.00%), and fourth in DR (92.86%). PBILMLP ranked third in DR (94.89%), fourth in ACC (96.65%), and ninth in FAR (0.0253). The PSOMLP algorithm ranked fifth in both ACC and DR while securing third place in FAR (0.0109). The MFOMLP algorithm was ranked sixth in ACC (95.95%), fifth in DR (91.07%), and seventh in FAR (0.0176). Further down the rankings, the HSMLP algorithm was placed seventh in both ACC and DR, and eighth in FAR, achieving rates of 94.29%, 87.50%, and 0.0252, respectively. Further down the list, the ESMLP algorithm also ranked eighth in both ACC and DR, and fourth in FAR, with rates of 92.65%, 79.39%, and 0.0112, respectively. Finally, the ABCMLP algorithm ranked ninth in both ACC and DR, and sixth in FAR, with rates of 89.32%, 70.14%, and 0.0168, respectively.

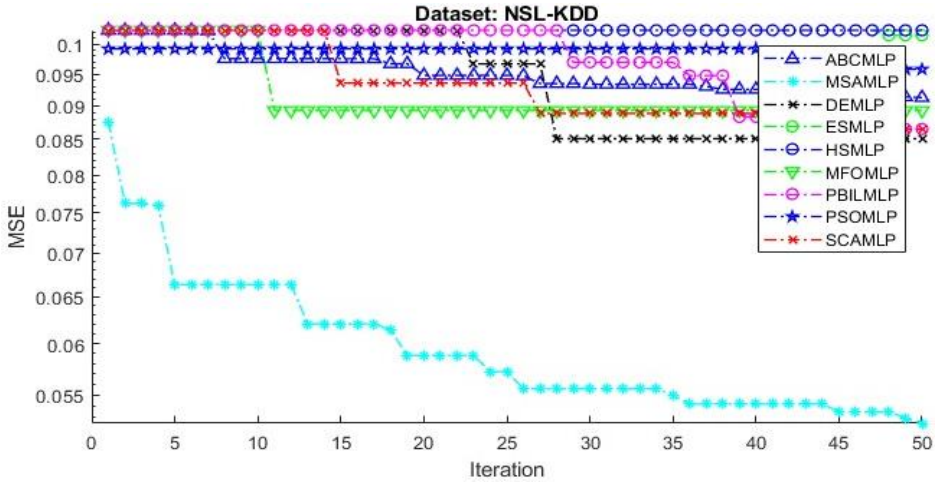


Figure 2. The performance measurements for 9 models compared to the NSL-KDD

Table 5. Performance classification across 9 algorithms in the UNSW-NB15 dataset

Algorithms	Accuracy	DR	FAR	MCC	Sensitivity	Specificity	F1	G mean
ABC	89.32	70.14	0.0168	0.75	0.70	0.98	0.81	83.05
MSA	98.93	98.21	0.0074	0.98	0.98	0.99	0.98	98.74
DE	97.83	96.43	0.0151	0.95	0.96	0.98	0.97	97.45
ES	92.65	79.39	0.0112	0.83	0.79	0.99	0.87	88.60
HS	94.29	87.50	0.0252	0.87	0.88	0.97	0.91	92.36
MFO	95.95	91.07	0.0176	0.91	0.91	0.98	0.93	94.59
PBIL	96.65	94.89	0.0253	0.92	0.95	0.97	0.95	96.17
PSO	96.41	91.07	0.0109	0.92	0.91	0.99	0.94	94.91
SCA	97.00	92.86	0.0106	0.93	0.93	0.99	0.95	95.85

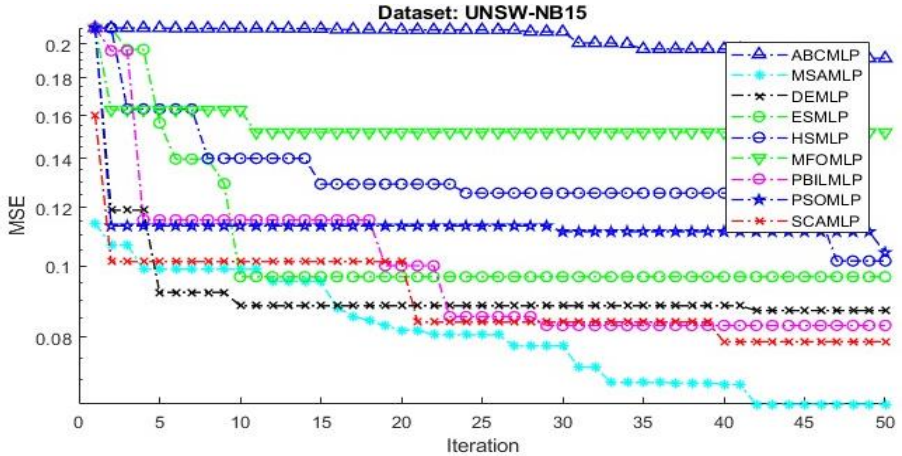


Figure 3. The performance measurements for nine models compared to the UNSW-NB15

Figure 3 illustrates the comparative results between MSAMLP and various other algorithms used to the UNSW-NB15 dataset. The analysis focuses on the convergence speed of MSE towards the final algorithmic output. Upon examining the convergence curves, it becomes evident that MSAMLP outperforms other algorithms in terms of convergence speed. This observation underscores the efficacy of the proposed.

5.3. Scenario 3: comparison of performance between proposed methods and others

In scenario 3, we evaluated our model against the latest IDS systems in Table 6 using six advanced techniques [11]–[15] on both datasets. Table 6 highlights its superior accuracy compared to previous studies, demonstrating its effectiveness. By integrating MSA with MLP, our model enhances adaptability and classification precision over traditional static methods. Future research could explore real-time anomaly detection, adaptive learning, and feature selection to further optimize IDS performance while minimizing computational costs for practical deployment.

Despite the promising results, applying the MSAMLP model in real-world IoT environments introduces several challenges. One primary concern is the computational limitations of IoT devices, as most have constrained processing power and memory capacity. This limitation necessitates the adoption of optimization techniques such as model compression, federated learning, and dynamic feature selection to maintain high detection accuracy while minimizing computational overhead.

Table 6. Assessing the outcomes of the suggested IDS techniques against alternative methods

Reference	Dataset	Model	Results
[11]	UNSW- NB15	MLP	84
[12]		LSTM	92
[13]		LR, DT, RF	92, 93, 95
Our proposed		MSAMLP	98.32
[13]	NSL-KDD	LR, DT, RF	90, 92, 94
[14]		KNNPSO-XGBoost	96, 95
[15]		SVM	96
Our proposed		MSAMLP	98.93

6. CONCLUSION

This study introduced an innovative IDS model called MSAMLP, focusing on applying MSA to train MLP effectively. The effectiveness of MSAMLP was evaluated in relation to contemporary IDS approaches, utilizing eight metaheuristic algorithms to optimize the training of the MLP. MSAMLP achieved impressive classification accuracies of 98.32% and 98.93% on both datasets, with DRs of 97.48% and 98.21%, and FARs of 0.0057 and 0.0074, respectively. These outcomes surpassed those of other models tested on the same datasets, showcasing MSAMLP's potential for practical IDS applications. However, the evaluation was limited to all features of the IDS dataset. Our findings provide conclusive evidence that MSAMLP enhances IDS performance by achieving superior accuracy and detection rates while maintaining low false alarm rates. However, the evaluation was limited to all features of the IDS dataset, suggesting the need for future studies to explore feature selection techniques and real-time deployment scenarios to further improve efficiency and adaptability in practical cybersecurity environments.

ACKNOWLEDGEMENTS

This research was supported by the Universiti Malaysia Terengganu (UMT/TAPE RG 2020/55225) and Artificial Intelligence Research Interest Group (AIRIG), also supported by the center of research excellence and incubation management (CRIEM) and artificial intelligence for sustainability and islamic research special interest group of Universiti Sultan Zainal Abidin, Terengganu, Malaysia.

FUNDING INFORMATION

This his research was supported by the center of research excellence and incubation management (CRIEM) and artificial intelligence for sustainability and Islamic research special interest group of Universiti Sultan Zainal Abidin, Terengganu, Malaysia.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Sanaa A. A. Ghaleb	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Mumtazimah Mohamad	✓	✓	✓	✓	✓	✓	✓				✓	✓	✓	✓
Waheed Ghanem	✓	✓	✓	✓	✓	✓	✓				✓			
Amir Ngah								✓	✓		✓			
Farizah Yunus				✓				✓	✓					
Arifah Che Alhadi					✓			✓	✓					
MD Nurul Islam Siddique										✓				

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

Data availability does not apply to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] N. Charef, A. Ben Mnaouer, M. Aloqaily, O. Bouachir, and M. Guizani, "Artificial intelligence implication on energy sustainability in internet of things: a survey," *Information Processing and Management*, vol. 60, no. 2, p. 103212, Mar. 2023, doi: 10.1016/j.ipm.2022.103212.

[2] T. Mahmud, M. A. H. Prince, M. H. Ali, M. S. Hossain, and K. Andersson. "Enhancing cybersecurity: Hybrid deep learning approaches to smishing attack detection." *Systems (MDPI)*, vol. 12, no. 11, pp. 490, 2024, doi: 10.3390/systems12110490.

[3] M. M. Rahman, S. Al Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," *Cyber Security and Applications*, vol. 3, p. 100082, Dec. 2025, doi: 10.1016/j.csa.2024.100082.

[4] R. Buchta, G. Gkoktsis, F. Heine, and C. Kleiner. "Advanced persistent threat attack detection systems: A review of approaches, challenges, and trends." *Digital Threats: Research and Practice*, vol. 5, no. 4, pp. 1-37, 2024, doi: 10.1145/3696014.

[5] O. Alamu, T. O. Olwal, and E. M. Migabo, "Machine learning applications in energy harvesting internet of things networks: a review," *IEEE Access*, vol. 13, pp. 4235–4266, 2025, doi: 10.1109/ACCESS.2024.3525263.

[6] N. J. Singh, N. Hoque, K. R. Singh, and D. K. Bhattacharyya. "Botnet-based IoT network traffic analysis using deep learning." *Security and Privacy*, vol. 7, no. 2, pp. e355, 2024, doi: 10.1002/spy2.355.

[7] M. J. Kumar, S. Mishra, E. G. Reddy, M. Rajmohan, S. Murugan, and N. A. Vignesh, "Bayesian decision model based reliable route formation in internet of things," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 34, no. 3, pp. 1665–1673, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1665-1673.

[8] Y. NarasimhaRao, P. Surya Chandra, V. Revathi, and N. S. Kumar, "Providing enhanced security in IoT based smart weather system," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 18, no. 1, pp. 9–15, Apr. 2019, doi: 10.11591/ijeecs.v18.i1.pp9-15.

[9] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: a survey," *Internet of Things (Netherlands)*, vol. 19, p. 100568, Aug. 2022, doi: 10.1016/j.iot.2022.100568.

[10] L. Liu, Z. Sajid, C. Kravaris, and F. Khan. "Detection and analysis of cybersecurity challenges for processing systems." *Process Safety and Environmental Protection*, vol. 185, pp. 1061-1071, 2024, doi: 10.1016/j.psep.2024.03.088.

[11] Y. Yin *et al.*, "IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset," *Journal of Big Data*, vol. 10, no. 1, p. 15, Feb. 2023, doi: 10.1186/s40537-023-00694-8.

[12] H. R. Sayegh, W. Dong, and A. M. Al-madani, "Enhanced intrusion detection with LSTM-based model, feature selection, and SMOTE for imbalanced data," *Applied Sciences (Switzerland)*, vol. 14, no. 2, p. 479, Jan. 2024, doi: 10.3390/app14020479.

[13] O. B. J. Rabie, S. Selvarajan, T. Hasanin, A. M. Alshareef, C. K. Yogesh, and M. Uddin, "A novel IoT intrusion detection framework using decisive red fox optimization and descriptive back propagated radial basis function models," *Scientific Reports*, vol. 14, no. 1, pp. 1–20, Jan. 2024, doi: 10.1038/s41598-024-51154-z.

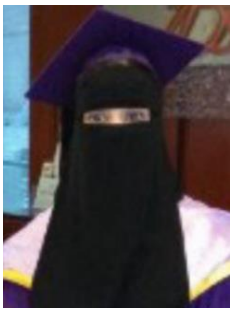
[14] M. Karthikeyan, D. Manimegalai, and K. RajaGopal, "Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection," *Scientific Reports*, vol. 14, no. 1, p. 231, Jan. 2024, doi: 10.1038/s41598-023-50554-x.

[15] Z. Good *et al.*, "Comparative analysis of machine learning techniques for IoT anomaly detection using the NSL-KDD dataset," *IJCSNS International Journal of Computer Science and Network Security*, vol. 23, no. 1, pp. 46–52, 2023, doi: 10.22937/IJCSNS.2023.23.1.7.

[16] M. Catillo, A. Pecchia, and U. Villano, "A deep learning method for lightweight and cross-device IoT botnet detection †," *Applied Sciences (Switzerland)*, vol. 13, no. 2, p. 837, Jan. 2023, doi: 10.3390/app13020837.

[17] Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, "A deep learning model for network intrusion detection with imbalanced data," *Electronics (Switzerland)*, vol. 11, no. 6, p. 898, Mar. 2022, doi: 10.3390/electronics11060898.
[18] G. G. Wang, "Moth search algorithm: a bio-inspired metaheuristic algorithm for global optimization problems," *Memetic Computing*, vol. 10, no. 2, pp. 151–164, Sep. 2018, doi: 10.1007/s12293-016-0212-3.
[19] W. A. H. M. Ghanem and A. Jantan, "A cognitively inspired hybridization of artificial bee colony and dragonfly algorithms for training multi-layer perceptrons," *Cognitive Computation*, vol. 10, no. 6, pp. 1096–1134, Sep. 2018, doi: 10.1007/s12559-018-9588-3.
[20] S. A. A. Ghaleb, M. Mohamad, S. A. Fadzli, and W. A. H. M. Ghanem, "Training neural networks by enhance grasshopper optimization algorithm for spam detection system," *IEEE Access*, vol. 9, pp. 116768–116813, 2021, doi: 10.1109/ACCESS.2021.3105914.
[21] W. A. H. M. Ghanem and A. Jantan, "Training a neural network for cyberattack classification applications using hybridization of an artificial bee colony and monarch butterfly optimization," *Neural Processing Letters*, vol. 51, no. 1, pp. 905–946, Oct. 2020, doi: 10.1007/s11063-019-10120-x.
[22] S. A. A. Ghaleb, M. Mohamad, S. A. Fadzli, and W. A. H. M. Ghanem, "E-mail spam classification using grasshopper optimization algorithm and neural networks," *Computers, Materials and Continua*, vol. 71, no. 2, pp. 4749–4766, 2022, doi: 10.32604/cmc.2022.020472.
[23] "NSL-KDD-DataSet," *Kaggle*. [Online]. Available: https://github.com/HoaNP/NSL-KDD-DataSet (accessed Jul. 20, 2016).
[24] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, Jan. 2016, doi: 10.1016/j.jnca.2015.11.016.
[25] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*, Nov. 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.

BIOGRAPHIES OF AUTHORS



Sanaa A. A. Ghaleb received the bachelor's degree from the University of Aden, Yemen, in 2011, and the M.Sc. degree from Universiti Sains Malaysia, Malaysia, in 2017. She received the Ph.D. degree from the Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Malaysia. Her research interests include technology-enhanced learning, instructional design and technology, computer networks and information security, cybersecurity, ML, AI, swarm intelligence, and metaheuristic. She can be contacted at email: sanaaghaleb.sg@gmail.com.

Mumtazimah Mohamad was born in Terengganu, Malaysia. She received the bachelor's degree in information technology from Universiti Kebangsaan Malaysia, in 2000, the M.Sc. degree in computer science from Universiti Putra Malaysia, and the Ph.D. degree in computer science from Universiti Malaysia Terengganu, in 2014. She was a Junior Lecturer, in 2000. Currently, she is an Associate Professor with the Department of Computer Science, Faculty of Informatics and Computing (FIK), Universiti Sultan Zainal Abidin, Terengganu, Malaysia. She has published over 50 research articles in peer-reviewed journals, book chapters, and proceeding. She has appointed a reviewer and technical committee for many conferences and journals and worked as a researcher in several national funded research and development projects. Her research interests include pattern recognition, machine learning, artificial intelligence, and parallel processing. She can be contacted at email: mumatazi@unisza.edu.my.

Waheed Ghanem received his B.Sc. degree in computer science and engineering from Aden University, Yemen, and later obtained both his M.Sc. degree in computer science (cybersecurity) and Ph.D. in cybersecurity from Universiti Sains Malaysia. His research interests focus on computer and network security, cybersecurity, artificial intelligence, swarm intelligence, metaheuristic algorithms, and information technology. His work explores advanced optimization techniques and AI-driven security solutions to enhance cybersecurity frameworks and intelligent computing systems. He can be contacted at email: waheed.ghanem@gmail.com.

Amir Ngah received the Ph.D. degree from Durham University, U.K., in 2012. He is currently an Associate Professor with the Faculty of Computer Science and Mathematics, Universiti Malaysia Terengganu. He has published more than 20 research papers at various refereed journals, conferences, seminars, and symposiums. His research interest includes on software engineering field, specifically in software testing, regression testing, software changes, software maintenance, software metrics, program analysis, and program slicing. He is also interested in AI and machine learning to assist in research in software engineering. He can be contacted at email: amir.ngah@gmail.com.

Farizah Yunus received the B.Sc. degree in electrical engineering (telecommunication) and the Ph.D. degree in telecommunication engineering from Universiti Teknologi Malaysia (UTM). She is currently a Senior Lecturer in computer science with the Faculty of Computer Science and Mathematics, University Malaysia Terengganu (UMT). Her specializes in networking, with a particular focus on wireless sensor networks, the IoT, cybersecurity, and cloud computing. She is a member of MBOT and BEM. She has worked as researcher in several national funded R&D projects. She can be contacted at email: farizah.yunus@gmail.com.

Arifah Che Alhadi received her B.Sc. with honors in information science from Universiti Kebangsaan Malaysia in 2001. She obtained her M.Sc. in information technology from the same university in 2005. Additionally, she earned her Ph.D. in computer science from Universiti Malaysia Terengganu in 2019. She currently holds a position as a senior lecturer in the Faculty of Computer Science and Mathematics at Universiti Malaysia Terengganu, Malaysia. Her research interests encompass information retrieval and information systems. She can be contacted at email: alhadi@gmail.com.

MD Nurul Islam Siddique studied civil engineering at the Khulna University of Engineering and Technology, Bangladesh, and graduated as MS in 2012 from University Malaysia Pahang. He then joined the research group of Prof. Zularisam at the Institute of University Malaysia Pahang. He received her Ph.D. degree in 2015 at the same institution. After that, he obtained the position of Assistant Professor at the University Malaysia Pahang. She has published more than 40 research articles in ISI journals. He can be contacted at email: md.nurul@gmail.com.