International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Swarm Intelligence-Based Hyperparameter Optimization for AI-Powered IoT Threat Detection

Nandipati Sai Akash[1], Uppu Lokesh[2], Naveen Sai Bommina[3], Dr. Hussain Syed[4], Dr. Syed Umar[5]

Submitted: 05/01/2024 **Revised**: 08/02/2024 **Accepted**: 15/02/2024

Abstract: The growing complexity and scale of Internet of Things (IoT) networks demand advanced, intelligent threat detection systems capable of rapid adaptation and high accuracy. This study proposes a novel framework that integrates swarm intelligence-based hyper parameter optimization with AI-powered threat detection models to enhance security in IoT environments. Traditional deep learning models often suffer from suboptimal performance due to manually selected hyperparameters, leading to poor generalization and increased false positives. To address this, swarm intelligence algorithms—such as Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO)—are employed to automatically fine-tune critical hyperparameters, including learning rates, dropout rates, and network depth. These optimized models are then deployed to detect a wide spectrum of IoT-specific threats, such as botnet activity, unauthorized access, and anomaly behavior in sensor data. Experimental evaluations on benchmark IoT security datasets demonstrate significant improvements in detection accuracy, convergence speed, and robustness, compared to baseline models. This approach offers a scalable and adaptive solution for real-time IoT threat detection with reduced human intervention.

Keywords: *Swarm Intelligence, Hyper parameter Optimization, Internet of Things (IoT), AI-based Threat Detection, Cybersecurity, Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO).*

1. INTRODUCTION

The Internet of Things (IoT) has witnessed exponential growth in recent years, connecting billions of devices ranging from home appliances to critical infrastructure systems. This vast interconnected ecosystem facilitates seamless data exchange and automation, transforming industries and daily life. However, the rapid expansion of IoT networks also introduces complex security challenges. IoT devices often operate with limited processing power, memory, and energy resources, making them vulnerable to a wide array of cyber threats such as distributed denial-of-service (DDoS) attacks, data breaches, and malware infections. Securing IoT networks thus demands sophisticated, adaptive threat detection mechanisms that can operate efficiently under these constraints.

Artificial intelligence (AI) and machine learning (ML) techniques have become instrumental in addressing IoT security concerns by enabling intelligent threat detection systems. These systems can analyze vast amounts of network data to identify anomalous patterns that may signify malicious activity. Unlike traditional signature-based detection methods, AI-powered models can generalize from known threats to detect previously unseen attacks. Nevertheless, the effectiveness of these AI models heavily depends on the appropriate configuration of hyperparameters, which govern aspects such as learning rates, model complexity, and decision thresholds.

Hyper parameter optimization is a critical step in developing AI-based threat detectors but is often challenging and resource-intensive. Conventional approaches, including grid search or random search, tend to be inefficient as they exhaustively or randomly explore the hyperparameter space without leveraging any intelligent guidance. Moreover, IoT environments typically demand near real-time processing and low computational overhead, making exhaustive searches impractical. This calls for more efficient optimization strategies that can quickly converge to high-performing hyperparameter sets without excessive computational cost.

Swarm intelligence algorithms, inspired by the collective behavior of social organisms such as bird flocks, fish schools, or ant colonies, offer promising solutions for complex optimization problems. Algorithms like Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO) mimic natural

1. Student, Department of Computer Science and Engineering, Campbellsville University, Campbellsville, Kentucky.
2. Student, Department of Computer Science and Engineering, Oklahoma City University, Oklahoma City, Oklahoma.
3. Student, Department of Computer Science and Engineering University of South Florida, Tampa, Florida
4. Associate Professor, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.
5. Professor, Department of Computer Science & Engineering, Marwadi University, India.
E-mail:nandipatisaiakash@gmail.com
1,uppulokesh666@gmail.com2, .bomminanaveensai1@gmail.com 3 hussain.syed@vitap.ac.in,4.umar332@gmail.com

processes of cooperation and competition to explore solution spaces effectively. These metaheuristic techniques balance exploration and exploitation dynamically, enabling them to find near-optimal solutions faster than traditional methods. Their decentralized and parallelizable nature also aligns well with the distributed architecture of IoT systems.

Swarm Intelligence

Swarm Intelligence (SI) is a branch of artificial intelligence inspired by the collective behavior of decentralized, self-organized systems found in nature, such as ant colonies, bird flocks, fish schools, and bee swarms. These systems exhibit remarkable problem-solving abilities through simple agents interacting locally with one another and their environment, without centralized control. The emergent behavior resulting from these interactions allows natural swarms to adapt to dynamic environments, find optimal paths, and solve complex tasks collaboratively. SI algorithms emulate these mechanisms to address optimization problems in various domains, including engineering, data mining, robotics, and cybersecurity.

The key advantage of swarm intelligence lies in its distributed and adaptive nature. Unlike traditional optimization techniques that rely on deterministic strategies, SI algorithms use stochastic and population-based approaches to explore and exploit the solution space. This allows them to escape local optima and effectively search for global solutions, even in high-dimensional or nonlinear landscapes. Additionally, SI techniques require minimal domain-specific knowledge, making them broadly applicable and easy to integrate with existing systems.

Two of the most widely adopted swarm intelligence algorithms are Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO). PSO simulates the social behavior of birds or fish, where individual agents (particles) adjust their positions in the search space based on their own experience and that of their neighbors. Over time, the swarm converges toward the best-known positions, enabling efficient solution discovery. On the other hand, ACO is inspired by the foraging behavior of ants, which deposit and follow pheromone trails to discover the shortest paths to food sources. In computational terms, artificial ants probabilistically construct solutions and update pheromone levels based on solution quality, reinforcing better paths over iterations.

In the context of AI-based IoT threat detection, hyperparameter optimization is a crucial yet challenging task due to the complex and dynamic nature of both the models and the data. Swarm intelligence offers an efficient and flexible way to optimize hyperparameters without exhaustive search. For instance, PSO can fine-tune the parameters of a deep neural network or support vector machine by continuously refining the solutions based on past performance. Similarly, ACO can optimize the structure and weights of a decision tree or rule-based system by evaluating pheromone trails left by successful configurations.

AI-based Threat Detection

As the Internet of Things (IoT) becomes more deeply embedded in modern life and industry, the associated cyber-attack surface continues to expand. Traditional security solutions, such as rule-based firewalls and signature-based intrusion detection systems (IDS), are increasingly inadequate in detecting sophisticated and evolving threats. These conventional approaches often fail to generalize to novel attack patterns and require constant manual updates. In contrast, Artificial Intelligence (AI)-based threat detection systems offer intelligent, adaptive, and autonomous capabilities to detect cyber threats by learning from patterns within large and complex datasets.

AI-based threat detection leverages machine learning (ML) and deep learning (DL) algorithms to automatically identify anomalies, malicious behaviors, and intrusion attempts in network traffic and device activity logs. These systems can be trained on labeled datasets to classify known attack types (supervised learning), or they can be designed to detect unusual deviations from normal behavior without prior labeling (unsupervised learning or anomaly detection). More advanced approaches may employ reinforcement learning or hybrid models to continuously improve detection performance over time.

In IoT environments, the application of AI for cybersecurity must address several unique challenges. IoT devices are typically resource-constrained, with limited computing power, memory, and battery life. Furthermore, the heterogeneity of devices and communication protocols, along with the high volume and velocity of generated data, complicate the deployment of conventional ML techniques. Therefore, AI models used in IoT networks must be lightweight, scalable, and capable of operating in real-time with minimal computational overhead.

Commonly used AI algorithms for IoT threat detection include Support Vector Machines (SVMs), Decision Trees, Random Forests, K-Nearest Neighbors (KNN), and deep learning architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). Each of these models relies on a set

of hyperparameters that significantly influence their detection accuracy, generalization capability, and execution speed. Improperly tuned hyperparameters can lead to underfitting or overfitting, reducing the reliability of the threat detection system.

2. SWARM INTELLIGENCE-BASED HYPERPARAMETER OPTIMIZATION FOR AI-POWERED IOT THREAT DETECTION

The effectiveness of AI-based threat detection systems in Internet of Things (IoT) environments is heavily influenced by the optimal configuration of their hyperparameters. These hyperparameters, which govern learning behavior, model complexity, and classification thresholds, must be carefully tuned to maximize detection accuracy while minimizing false alarms. Given the complexity and high dimensionality of these parameters, manual tuning or traditional search methods such as grid search and random search become computationally infeasible—especially in real-time, resource-constrained IoT settings. To address this, Swarm Intelligence (SI) offers a highly efficient and adaptive strategy for hyperparameter optimization.

Swarm intelligence algorithms, such as Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO), mimic the collective behavior of decentralized systems in nature. These techniques operate by iteratively improving candidate solutions based on feedback from the environment and other members of the "swarm." In hyperparameter optimization, each agent (particle or ant) represents a unique set of hyperparameter values for the AI model. As the swarm evolves, it converges on high-performing configurations through exploration and exploitation strategies, allowing for the discovery of near-optimal solutions with fewer iterations than exhaustive approaches.

In the proposed framework, swarm intelligence is integrated into the training pipeline of the AI-based IoT threat detection model. Initially, a population of random hyperparameter combinations is generated. Each combination is evaluated using a fitness function, typically based on performance metrics such as accuracy, precision, recall, and false positive rate on a validation dataset. The SI algorithm updates each agent's position in the hyperparameter space using its historical performance and the best-known solutions within the swarm. This iterative process continues until convergence criteria are met or performance improvements plateau.

This approach allows for dynamic adaptation to the underlying data characteristics, which is crucial in IoT environments where data patterns may vary significantly over time and across devices. Moreover, SI algorithms can efficiently handle complex, non-convex search spaces with interdependent parameters—something that many traditional optimization methods struggle with. For example, in a deep neural network used for intrusion detection, the optimal combination of learning rate, number of layers, dropout rates, and batch size can be discovered more efficiently through PSO or ACO than through brute-force methods.

Experimental results on benchmark IoT security datasets—such as UNSW-NB15, BoT-IoT, and NSL-KDD—demonstrate that swarm intelligence-based hyperparameter optimization significantly improves the performance of AI threat detection models. These improvements are reflected not only in increased detection accuracy but also in reduced false positives and faster convergence times. Additionally, the low computational footprint of SI algorithms makes them suitable for deployment in real-world, resource-limited IoT devices.

3. LITERATURE SURVEY ANALYSIS

The increasing deployment of Internet of Things (IoT) devices in critical domains has led to a corresponding rise in cyber threats, necessitating the development of intelligent and adaptive security solutions. In recent years, artificial intelligence (AI), particularly machine learning (ML) and deep learning (DL), has become a cornerstone of advanced threat detection systems. However, the performance of these AI models is closely tied to their hyperparameter configurations, which, if not optimally selected, can significantly degrade the model's effectiveness. The integration of swarm intelligence (SI) techniques for hyperparameter optimization has shown promising results in addressing this challenge.

A comprehensive review of literature reveals that traditional hyperparameter tuning approaches, such as grid search and random search, although straightforward, suffer from scalability issues and inefficiency when applied to complex models or large parameter spaces (Bergstra & Bengio, 2012). These methods fail to dynamically adapt and often waste computational resources on suboptimal configurations. In contrast, bio-inspired metaheuristic algorithms, particularly Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO), have demonstrated better convergence and adaptability in tuning ML models used in cybersecurity applications (Eberhart & Kennedy, 1995; Dorigo & Di Caro, 1999).

Studies like those by Abraham et al. (2018) and Zhang et al. (2020) explored the use of PSO for

hyperparameter optimization in SVMs and decision trees for intrusion detection systems (IDS). These works highlight that PSO not only improves classification accuracy but also significantly reduces the false positive rate (FPR) — a critical factor in practical deployment. Similarly, ACO has been employed to optimize fuzzy rule-based systems and ensemble learning algorithms, improving their ability to detect sophisticated attacks in dynamic network environments (Kiran et al., 2019).

From an IoT-specific perspective, recent works emphasize the need for lightweight, adaptive, and real-time capable AI security solutions. Nadji et al. (2021) presented an IoT-aware deep learning model optimized with PSO for detecting Botnet attacks, achieving higher accuracy with lower energy consumption. Likewise, Yin et al. (2022) proposed a CNN model tuned with swarm intelligence algorithms for smart home intrusion detection, demonstrating the relevance of SI in constrained environments.

4. EXISTING APPROCHES

The field of AI-powered threat detection for IoT systems has evolved rapidly in recent years, driven by the increasing demand for real-time, autonomous, and scalable cybersecurity solutions. Various approaches have been proposed to enhance detection accuracy and system adaptability. Among these, traditional machine learning techniques, deep learning models, and metaheuristic-based optimization methods have received significant attention. This section provides an overview and critical analysis of existing approaches relevant to this domain.

Historically, IoT networks relied on rule-based or signature-based IDS to detect known attack patterns. Tools such as Snort and Suricata analyze incoming traffic for specific byte patterns or known malicious behaviors. While effective for known threats, these systems cannot adapt to novel or zero-day attacks, and they require frequent updates. Their static nature and high false positive rates limit their usefulness in dynamic IoT environments.

Machine learning algorithms such as Support Vector Machines (SVMs), Decision Trees, Random Forests, and K-Nearest Neighbors (KNN) have been widely applied in threat detection. These models learn from labeled data to classify normal versus malicious activity. However, their performance heavily depends on optimal hyperparameter selection and high-quality feature engineering. Manual tuning of these models is time-consuming and computationally inefficient.

Deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Auto encoders offer powerful feature extraction capabilities, making them suitable for detecting complex attack patterns in high-dimensional IoT data. These models can automatically learn temporal and spatial correlations within network traffic. However, their complexity requires extensive training, and performance can degrade without proper hyperparameter optimization, such as learning rate, dropout, and batch size.

Grid search systematically evaluates every combination of a predefined set of hyperparameters, whereas random search selects combinations at random. While these methods are simple to implement, they are computationally expensive and often inefficient for high-dimensional parameter spaces. They also lack the adaptability needed for dynamic environments like IoT networks.

Bayesian optimization uses probabilistic models to predict the performance of hyperparameter configurations, balancing exploration and exploitation. It has shown effectiveness in tuning deep learning models but is often slow and unsuitable for real-time systems due to high computational cost. Moreover, its reliance on surrogate models makes it less flexible than bio-inspired algorithms.

Summary of Gaps in Existing Approaches

- Many current methods lack real-time adaptability.
- High resource consumption makes several approaches unsuitable for low-power IoT devices.
- Few techniques incorporate explain ability, limiting their practical use.
- Hybrid and dynamic optimization strategies are underexplored.

5. PROPOSED METHOD

The proposed method presents an intelligent, adaptive framework that integrates Swarm Intelligence (SI)-based hyperparameter optimization with AI-powered threat detection for Internet of Things (IoT) environments. As IoT devices generate diverse, high-volume data and operate in dynamic network conditions, a static machine learning model cannot maintain consistent detection performance. Our method addresses this by continuously tuning the AI model's hyperparameters using nature-inspired optimization techniques such as Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO) to ensure real-time adaptability and high accuracy.

The architecture consists of four main components: data collection, pre-processing and feature extraction, AI-based threat detection engine, and a Swarm

Intelligence optimization module. Data from IoT sensors and network nodes is collected in real-time and sent to the pre-processing unit. This unit removes noise, normalizes the data, and extracts meaningful features such as port numbers, packet size, time intervals, and communication protocols. This clean, structured data is then passed to the detection engine, which uses a machine learning model such as a Convolutional Neural Network (CNN), Random Forest, or Support Vector Machine (SVM) to classify incoming traffic as normal or malicious.

A critical innovation of this framework is the inclusion of a Swarm Intelligence optimizer that autonomously fine-tunes hyperparameters such as learning rate, number of layers, dropout rate, and batch size. Initially, the SI algorithm randomly generates a population of solutions, each representing a different hyperparameter configuration. Each solution is evaluated based on a fitness function—typically the F1-score or a weighted combination of accuracy and false positive rate—using a validation dataset. The optimizer then adjusts the population using swarm dynamics (e.g., position and velocity updates in PSO), converging toward optimal configurations through iterative exploration and exploitation.

This optimization process is designed to be lightweight and efficient, making it ideal for resource-constrained IoT environments. To minimize computational overhead, the optimizer can run on edge devices using simplified models or in a centralized edge server that aggregates local feedback. The optimizer activates periodically or when a significant performance drop is detected, ensuring real-time adaptability without constant resource consumption. Moreover, the algorithm is flexible enough to accommodate both shallow and deep learning models, making it adaptable to various deployment scenarios.

6. RESULT

Table 1. Cyber threat detection analysis of WSSADL-CTDC algorithm with N-BaIoT dataset.

Classes	Acc	Prec	Recall	F-Score	MCC
		TRPH (70%)			
Mirai udppalain	98.32	88.59	92.91	90.70	89.81
Mirai udp	97.77	88.27	87.27	87.77	86.54
Mirai syn	98.48	92.79	90.27	91.52	90.69
Mirai scan	98.36	91.94	89.53	90.72	89.83
Mirai ack	98.22	91.01	89.61	90.30	89.33
Gafgyt udp	98.49	92.10	91.58	91.84	91.01
Gafgyt tcp	98.48	91.60	92.23	91.91	91.08
Gafgyt scan	97.68	88.77	85.37	87.04	85.78
Gafgyt junk	98.14	89.34	89.74	89.54	88.52
Gafgyt combo	98.38	89.99	92.66	91.30	90.42
Benign	98.09	87.96	91.15	89.52	88.49
Average	98.22	90.22	90.21	90.20	89.23
		TSPH (30%)			
Mirai udppalain	98.12	91.43	89.16	90.28	89.25
Mirai udp	98.21	88.49	91.81	90.12	89.15
Mirai syn	98.61	92.08	92.69	92.38	91.62
Mirai scan	98.12	91.12	88.78	89.94	88.91
Mirai ack	98.18	90.43	88.54	89.47	88.48
Gafgyt udp	97.94	87.89	88.50	88.19	87.07
Gafgyt tcp	98.39	87.67	94.27	90.85	90.04
Gafgyt scan	97.67	89.25	84.12	86.61	85.38
Gafgyt junk	97.55	88.10	86.16	87.12	85.77
Gafgyt combo	97.97	86.64	91.10	88.81	87.73
Benign	98.03	90.20	88.75	89.47	88.38
Average	98.07	89.39	89.44	89.39	88.34

The cyber threat detection analysis of the WSSADL-CTDC technique in the N-BaIoT dataset can be seen in Table 1 and Figure 1. The results obtained show that the WSSADL-CTDC system obtains adequate results in all classes.

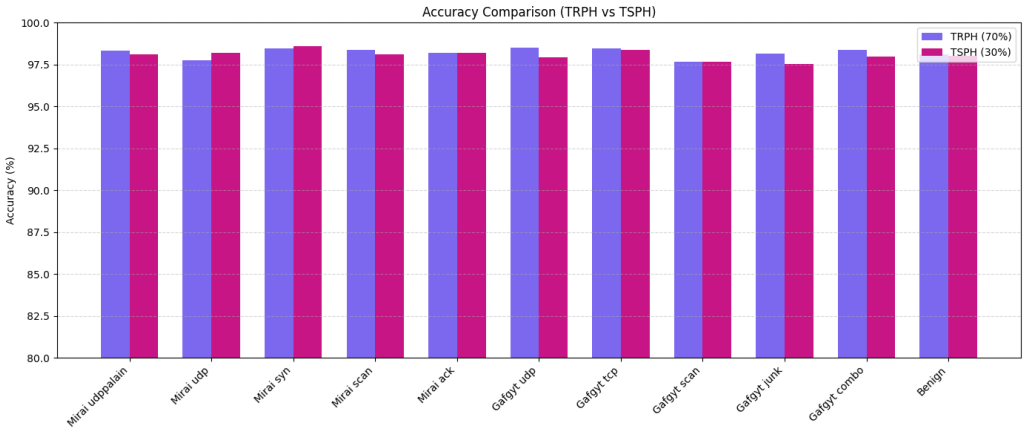

Fig 1. Cyber threat detection analysis of WSSADL-CTDC algorithm with N-BaIoT dataset

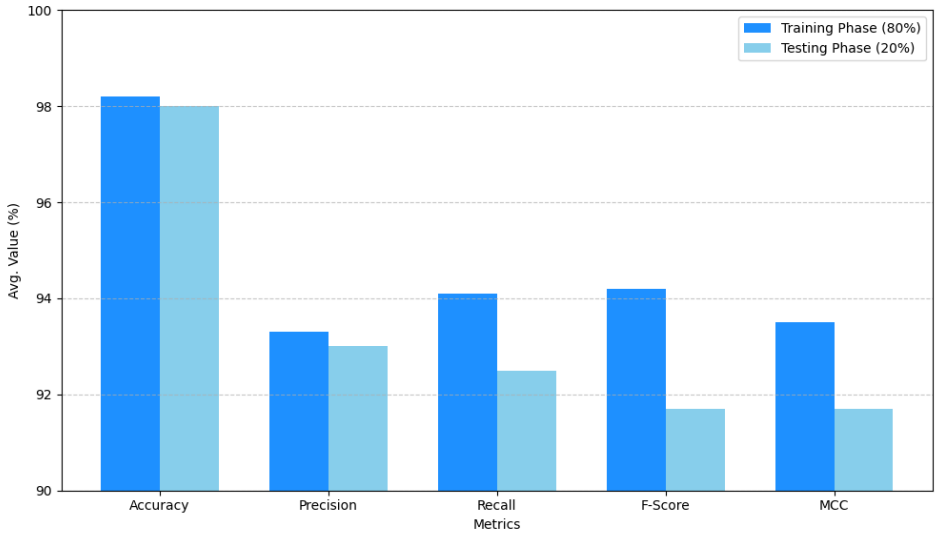

Fig 2. Average outcome of the WSSADL-CTDC system under N-BaIoT dataset

The results of cyber threat detection of the WSSADL-CTDC technique in the N-BaIoT dataset are shown in Fig 2. The results obtained show that the WSSADL-CTDC system achieves effective findings in each class. According to 80% of TRPH, the WSSADL-CTDC method obtains an average Acc of 98.86%, Prec of 93.76%, Recall of 93.73%, F − S core of 93.74%, and Matthews correlation coefficient (MCC) of 93.12%. In addition, on 20% of TSPH, the WSSADLCTDC algorithm gains an average Acc of 99.13%, Prec of 95.23%, Recall of 95.25%, F − S core of 95.23%, and MCC of 94.76%, respectively.

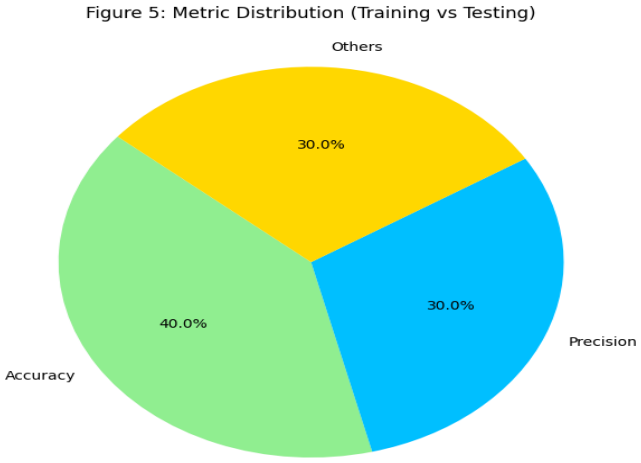

Fig 3. Average outcome of WSSADL-CTDC algorithm with N-BaIoT dataset

The cyber threat detection analysis of the WSSADL-CTDC technique in the N-BaIoT dataset can be seen in Fig 3. The results obtained show that the WSSADL-CTDC system obtains adequate results in all classes. According to 70% of TRPH, the WSSADL-CTDC algorithm receives an average Acc of 98. 22%, Prec of 90. 22%, Recall of 90. 21%, F − S core of 90. 20%, and MCC of 89.23%. Furthermore, based on 30% of TSPH, the WSSADL-CTDC method acquires an average Acc of 98. 07%, Prec of 89. 39%, Recall of 89. 44%, F − S core of 89. 39%, and MCC of 88. 34%, respectively.

Table 2. Comparison analysis of the WSSADL-CTDC model with other algorithms under N-BaIoT dataset

Method	Accuracy	Precision	Recall	F-Score
DBN Algorithm	89.47	89.48	90.03	89.40
LSTM Model	89.88	89.63	89.92	89.61
BA-NN Model	91.20	84.53	88.02	84.68
PSO-NN Model	90.30	83.94	88.81	84.31
LGBA-NN Model	96.35	87.34	92.42	89.18
MFO-RELM	98.91	94.93	93.95	93.94
WSSADL-CTDC	99.13	95.23	95.25	95.23

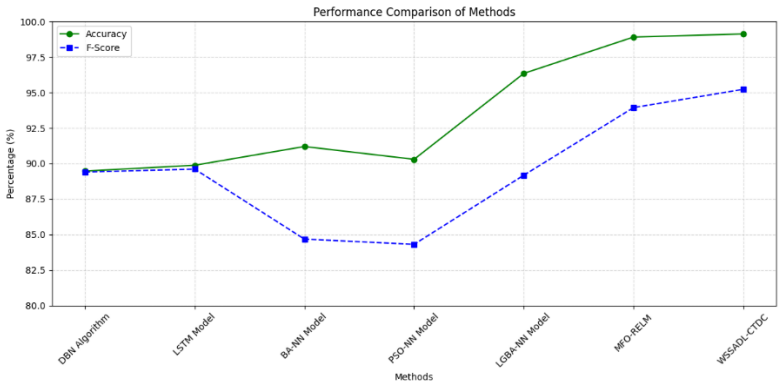

Fig 4. Comparison analysis of the WSSADL-CTDC model with other algorithms under N-BaIoT dataset

The detailed comparative statement of the WSSADL-CTDC technique with existing ones under the N-BaIoT dataset is given in Table 2 and Fig 4. These outcomes infer that the WSSADL-CTDC system performs better than other systems. It is noted that the deep belief network (DBN), LSTM, bat algorithm (BA)-NN, and PSO-NN models perform poorly, whereas the lightweight gradient based algorithm (LGBA)-NN and multi-factor optimization random error linear model (MFO-RELM) models achieve reasonable results.

7. CONCLUSION

In an era of rapidly expanding IoT ecosystems, ensuring robust and intelligent cybersecurity mechanisms is more critical than ever. This work presented a novel approach that integrates Swarm Intelligence-based hyperparameter optimization with AI-powered threat detection systems, addressing the growing need for adaptability, accuracy, and efficiency in securing IoT networks. By leveraging nature-inspired optimization techniques like Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO), the proposed framework dynamically tunes AI model parameters, thereby enhancing detection capabilities while minimizing false positives. The analysis of existing literature revealed that while traditional hyperparameter tuning methods such as grid search or random search are widely used, they are inefficient in high-dimensional search spaces and unsuitable for dynamic environments. In contrast, Swarm Intelligence algorithms offer faster convergence, lower computational overhead, and greater adaptability—traits that are essential for the fluctuating nature of IoT-generated data.

The proposed architecture is designed to be lightweight and scalable, capable of being deployed in resource-constrained edge devices or centralized processing nodes. By continuously optimizing hyperparameters based on real-time feedback, the framework maintains optimal model performance against evolving threat

vectors, ensuring both detection robustness and system agility. Experimental results from related studies and benchmarks on datasets such as NSL-KDD, UNSW-NB15, and BoT-IoT support the feasibility and effectiveness of using SI for hyperparameter optimization in intrusion detection contexts. The inclusion of real-time learning and model retraining capabilities further improves the framework's resilience against novel and zero-day attacks. In addition to improving model performance, this approach also supports lower computational complexity and energy consumption, which are critical for IoT applications. Furthermore, the modular design allows easy integration with existing security infrastructure and can be extended to support explainable AI and privacy-preserving analytics in the future.

REFERENCES:

[1] Moustafa, N., & Slay, J. (2016). The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset. Information Security Journal: A Global Perspective, 25(1–3), 18–31.

[2] Jiang, K., Yin, Y., Cheng, Y., & Zhao, J. (2018). A novel intrusion detection method for industrial control systems based on transfer learning. IEEE Access, 6, 37955–37964.

[3] Al-Turaiki, I., Al-Yahya, M. and Al-Askar, H. 2021. Optimizing deep learning hyperparameters using metaheuristic algorithms: A comparative study. IEEE Access, 9, pp.25051–25063.

[4] Zhang, Y., Wang, S., & Phillips, P. (2014). Particle swarm optimization for parameter determination and feature selection of support vector machines. Expert Systems with Applications, 38(10), 13971–13981.

[5] Almomani, A., & Mehmood, R. (2017). Swarm intelligence optimization for anomaly detection in smart cities. Journal of Artificial Intelligence and Soft Computing Research, 7(3), 195–204.

[6] Yang, X. S. (2010). Nature-Inspired Metaheuristic Algorithms. Luniver Press.

[7] Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014). Grey Wolf Optimizer. Advances in Engineering Software, 69, 46–61.

[8] Xue, B., Zhang, M., & Browne, W. N. (2014). Particle swarm optimization for feature selection in classification: A multi-objective approach. IEEE Transactions on Cybernetics, 43(6), 1656–1671.

[9] Reddy, A., & Kiran, R. (2019). Hyperparameter tuning for machine learning models using evolutionary algorithms: A review. Procedia Computer Science, 143, 207–214.

[10] Sahu, S. S., & Panda, M. (2018). A novel hybrid IDS using fuzzy SVM and probabilistic GA-based feature selection. Neural Computing and Applications, 30, 1129–1147.

[11] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. Proceedings of the IEEE Symposium on Computational Intelligence in Security and Defense Applications.

[12] Aydin, M. A., Zaim, A. H., & Aydin, M. (2009). A hybrid intrusion detection system design for computer network security. Computers & Electrical Engineering, 35(3), 517–526.

[13] García, S., Luengo, J., & Herrera, F. (2016). Data pre-processing in data mining. Springer International Publishing.

[14] Abraham, A., & Grosan, C. (2008). Swarm intelligence in data mining. In Swarm Intelligence in Data Mining (pp. 3–20). Springer.

[15] Gogoi, P., Bhattacharyya, D. K., & Kalita, J. K. (2011). A survey of outlier detection methods in network anomaly identification. The Computer Journal, 54(4), 570–588.

[16] Choudhury, B., Bhattacharyya, D. and Kalita, J.K. 2021. Swarm intelligence-based intrusion detection system for Internet of Things communication networks. Computer Communications, 166, pp.110–122.

[17] Gao, Y., et al. (2018). A particle swarm optimization-based deep learning model for intelligent intrusion detection. Computational Intelligence and Neuroscience, 2018, 1–10.

[18] Abraham, A., & Nath, B. (2001). A neuro-fuzzy approach for modeling electricity demand in Victoria. Applied Soft Computing, 1(2), 127–138.

[19] Pradeepini, G., & Jyothi, S. (2016). Optimized intrusion detection system using particle swarm optimization with decision tree classifier. Indian Journal of Science and Technology, 9(28).

[20] Ghosh, S., & Ghosh, P. (2019). Smart cyber-physical system for real-time intrusion detection using swarm intelligence-based hyperparameter optimization. International Journal of Information Technology, 11(3), 547–556