Journal of Theoretical and Applied Information Technology
15th July 2025. Vol.103. No.13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURING CYBER-PHYSICAL SYSTEMS: FLAMINGO SEARCH ALGORITHM OPTIMIZED DEEP LEARNING FOR THREAT DETECTION

K. SRI VIJAYA[1], S. SUDESHNA[2], NARESH KUMAR BHAGAVATHAM[3], PARASA KONDALA RAO[4], N. SRIJA[5], PRAVEENA MANDAPATI[6], RAMESH ELURI[7]

[1]Department of Information Technology, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India
[2]Department of Computer Science and Engineering, VNR Vignana Jyothi Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana, India
[3]Department of Computer Science and Engineering, Vignana Bharathi Institute of Technology, Ghatkesar, Hyderabad, Telangana, India
[4]Department of Electrical and Electronics Engineering, Aditya University, Surampalem, Andhra Pradesh, India
[5]Department of Information Technology, M. Kumarasamy College of Engineering, Karur, Tamilnadu, India
[6]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
[7]Department of Computer Science and Engineering, R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India

E-mail: srivijayak@gmail.com, sudeshna_s@vnrvjiet.in, bhagavatham.nareshkumar@vbithyd.ac.in, raoparasa455@gmail.com, srijanallathambi@gmail.com, praveena.conf@gmail.com, eluri.r@gmail.com

ABSTRACT

Threat detection in Cyber-Physical Systems (CPS) is essential to safeguarding the reliability and security of these integrated systems, which interface digital components with the physical world. CPS platforms, common in healthcare, industrial automation, smart cities, and transportation, face vulnerability to various cyber threats. Effective threat detection in CPS involves identifying and mitigating cybersecurity risks, which can otherwise disrupt physical operations, compromise data integrity, and jeopardize safety. Machine Learning (ML) and Deep Learning (DL) techniques are increasingly leveraged for detecting anomalies by modeling the CPS's normal behaviour and recognizing deviations. This study presents an Automated Threat Detection using the Flamingo Search Algorithm with Optimal Deep Learning (ATD-FSAODL) in CPS environments. Initially, the ATD-FSAODL technique applies Flamingo Search Algorithm (FSA)-based feature subset selection to identify optimal feature sets. The ATD-FSAODL approach utilizes a modified Elman Spike Neural Network (MESNN) for threat recognition and classification, with the Slime Mold Algorithm (SMA) optimizing the MESNN parameters to enhance detection accuracy. Simulation experiments on benchmark databases demonstrate the effectiveness of the ATD-FSAODL technique, achieving a maximum accuracy of 99.58%, precision of 99.58%, recall of 99.58%, F-score of 99.58%, and MCC of 99.16%.

Keywords: *Cyber-physical system, Threat analysis, Industry 4.0, Deep learning, Feature selection*

1. INTRODUCTION

Cyber-Physical Systems (CPS) represent a convergence of physical processes with computational capabilities, where embedded devices and communication networks enable seamless monitoring, control, and automation. Found in diverse applications like healthcare, industrial automation, smart cities, and transportation, CPS environments are fundamental to the efficiency and safety of modern infrastructure. However, the interconnected nature of CPS introduces substantial cybersecurity challenges. Cyber threats targeting CPS can

compromise data integrity, disrupt physical operations, and, in critical sectors, pose direct threats to safety and human lives [1], [2]. The detection of cyber threats in CPS is inherently complex. Unlike traditional IT systems, where security threats often manifest in the digital domain alone, CPS environments involve an interplay between the cyber and physical realms. Attacks on CPS systems can produce cascading effects, where a digital intrusion triggers undesirable physical behaviors, causing substantial disruption or damage. Thus, there is an urgent need for reliable and efficient threat detection frameworks tailored to CPS that can anticipate, detect, and mitigate these multifaceted threats in real time [3], [4]. Machine Learning (ML) and Deep Learning (DL) models are increasingly popular for anomaly detection in CPS due to their ability to model complex, nonlinear relationships. By learning the normal operational patterns of CPS, ML and DL models can identify deviations that may indicate security threats. Despite their potential, existing ML and DL techniques often face challenges with high-dimensional data, variable network dynamics, and the requirement for rapid, responsive analysis. Addressing these issues requires a comprehensive approach that integrates advanced feature selection and parameter optimization to maximize model efficiency and accuracy [5].

This study introduces a novel Automated Threat Detection using the Flamingo Search Algorithm with Optimal Deep Learning (ATD-FSAODL) framework, designed specifically for CPS environments [6]. The ATD-FSAODL model incorporates three primary components to achieve high-performance threat detection: Flamingo Search Algorithm (FSA) for Feature Selection: The FSA is used for selecting relevant features from high-dimensional CPS data. Inspired by flamingo foraging behavior, FSA offers a balanced approach to exploration and exploitation, identifying feature subsets that maximize detection accuracy [7].

Modified Elman Spike Neural Network (MESNN) for Threat Classification: The MESNN is a modified neural network designed to capture temporal data patterns in CPS environments. By integrating spike neurons, MESNN improves sensitivity to subtle anomalies, enhancing classification accuracy for different types of threats [8]. Slime Mold Algorithm (SMA) for Parameter Optimization: The SMA optimizes the MESNN's parameters to further enhance its accuracy. By mimicking the adaptive foraging behavior of slime molds, SMA achieves optimal parameter settings, ensuring the MESNN model is finely tuned to detect even low-signal threats effectively [9]. The ATD-FSAODL framework was evaluated on benchmark CPS datasets to validate its performance. Experimental results indicate that the proposed approach offers substantial improvements in threat detection accuracy, achieving an accuracy of 99.58%, with equally high precision, recall, and F-scores. These results demonstrate the model's capability in efficiently identifying threats and reducing false positives, making it well-suited for real-time applications in CPS environments [10].

In recent years, significant research has focused on developing effective threat detection mechanisms for Cyber-Physical Systems (CPS). Traditional cybersecurity methods are often insufficient for CPS, given the unique characteristics of these systems that require integration between digital and physical domains. This section provides a review of notable machine learning (ML), deep learning (DL), and optimization techniques applied in CPS threat detection, highlighting their strengths and limitations [11], [12]. Machine learning methods, including Support Vector Machines (SVM), Decision Trees (DT), and Random Forests (RF), are widely used in anomaly detection for CPS. For example, SVM has shown effectiveness in detecting boundary anomalies in complex CPS data, as it handles non-linearly separable data and performs well in high-dimensional spaces. However, SVM struggles with large datasets typical of CPS, leading to scalability issues and increased computational costs [13]. Other ML approaches, such as Random Forests and k-Nearest Neighbors (k-NN), are commonly applied in CPS environments due to their simplicity and interpretability. Nevertheless, these models lack the adaptability needed for rapidly evolving threat profiles. As a result, traditional ML models are frequently enhanced with feature selection techniques or combined with ensemble methods to improve performance, though this often comes at the cost of increased complexity and computational demand [14], [15].

Deep learning models, particularly Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), have gained popularity in CPS threat detection due to their ability to capture complex patterns and temporal dependencies within data. CNNs are typically employed to detect spatial patterns, while RNNs and Long Short-Term Memory (LSTM) networks are favored for sequence-based data, such as time-series data in CPS environments [16], [17]. While DL models

like LSTM and CNN offer high accuracy, their application in CPS is constrained by the high dimensionality of CPS data and the computational expense of training deep networks. This limitation can be critical in real-time environments, where fast detection and response are essential. Recent efforts have incorporated hybrid approaches that combine CNN and LSTM layers for enhanced feature extraction, yet these architectures can be difficult to train and fine-tune [18]. To improve the efficiency of ML and DL models in CPS threat detection, feature selection and parameter optimization have become important areas of research. Metaheuristic algorithms, such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and Ant Colony Optimization (ACO), have been employed to select the most relevant features and optimize model parameters [19]. PSO and GA are frequently used for parameter optimization, where they help reduce overfitting and improve model accuracy by optimizing hyperparameters. However, these algorithms can become trapped in local optima, particularly in high-dimensional spaces, limiting their effectiveness. Additionally, the convergence speed of PSO and GA can be slow, especially when dealing with the complex and dynamic threat profiles encountered in CPS environments [20]. Nature-inspired algorithms, such as the Flamingo Search Algorithm (FSA) and Slime Mold Algorithm (SMA), have emerged as promising alternatives for feature selection and optimization in CPS threat detection. FSA, inspired by the foraging behavior of flamingos, has demonstrated high efficiency in exploration and exploitation balance, making it suitable for selecting optimal feature subsets in high-dimensional data. FSA's lightweight computational nature enables it to identify key features that contribute to threat detection, enhancing model accuracy without excessive computational cost [21]. Similarly, the Slime Mold Algorithm (SMA) has shown potential for parameter optimization due to its adaptability and robustness. Unlike traditional algorithms, SMA dynamically adjusts its search behavior based on environmental conditions, allowing it to avoid local optima and improve convergence speed. The adaptive properties of SMA make it well-suited for CPS environments where threat patterns can shift unpredictably [22]. While significant progress has been made in applying ML, DL, and optimization algorithms for CPS threat detection, several gaps remain. First, the high-dimensional nature of CPS data often leads to computational inefficiencies and reduced detection accuracy. Many existing models struggle to balance detection performance with computational feasibility, particularly for real-time applications [23]. Moreover, few studies have explored hybrid approaches that integrate advanced feature selection, deep learning, and parameter optimization specifically tailored for CPS. While FSA and SMA offer promising solutions, they have not been widely tested in CPS environments. Furthermore, existing studies seldom focus on models capable of detecting a broad range of threat profiles while adapting to the dynamic nature of CPS [24].

To address these gaps, the proposed Automated Threat Detection using Flamingo Search Algorithm with Optimal Deep Learning (ATD-FSAODL) combines FSA for feature selection, a Modified Elman Spike Neural Network (MESNN) for threat detection, and SMA for parameter optimization. This hybrid approach leverages the strengths of each component to achieve a high-performance, computationally efficient solution suitable for CPS. By integrating FSA and SMA with MESNN, the ATD-FSAODL framework aims to provide a comprehensive and adaptable solution for automated threat detection in CPS environments [25]. In summary, while existing methods have laid a strong foundation for CPS threat detection, they often fall short in scalability, adaptability, and real-time performance. The ATD-FSAODL approach seeks to overcome these limitations, offering an efficient, accurate, and responsive solution tailored to the unique challenges of CPS threat detection. The following sections elaborate on the methodology, experimental setup, and performance evaluation of the proposed approach.

2. STYLE OF PAPER

The proposed Automated Threat Detection using Flamingo Search Algorithm with Optimal Deep Learning (ATD-FSAODL) methodology is designed to detect and classify threats in Cyber-Physical Systems (CPS) by effectively integrating feature selection, optimized deep learning, and parameter tuning. The methodology consists of three main components: feature subset selection using the Flamingo Search Algorithm (FSA), threat classification with the Modified Elman Spike Neural Network (MESNN), and parameter optimization using the Slime Mold Algorithm (SMA). Figure 1 illustrates the complete process of the ATD-FSAODL method [26].

Feature selection is critical in CPS environments due to the high dimensionality and variability of data generated by interconnected devices. The Flamingo Search Algorithm (FSA) is employed to reduce the data dimensionality by

selecting the most relevant features, thereby enhancing computational efficiency and model accuracy [27]. The Flamingo Search Algorithm (FSA) is an optimization technique inspired by the social behavior and foraging patterns of flamingos, particularly in their search for food in complex environments. FSA has emerged as a promising tool in optimization, and one of its practical applications is in feature selection in machine learning and data mining. Feature selection aims to identify the most informative subset of features that contribute to the performance of predictive models, reducing dimensionality, computational costs, and overfitting [28]. FSA operates on the principles of flamingo behavior, such as flocking, prey tracking, and food searching, which help flamingos find food in wetlands efficiently. The algorithm typically includes phases that simulate:

Foraging Behavior: Flamingos assess their environment to identify the areas with higher food density.

Tracking Prey: By observing other flamingos' positions, they refine their search to maximize food intake.

Decision-Making and Communication: Flamingos move in response to their surroundings and the actions of others, balancing exploration and exploitation.

This process can be adapted to optimization problems, where each "flamingo" represents a potential solution, and its position in the search space corresponds to a set of selected features. Steps of Feature Selection Using FSA

Initialization: Initialize a population of flamingos, where each flamingo is a candidate subset of features from the dataset. The quality of each subset is evaluated based on a fitness function, often accuracy or a performance metric of a classifier trained on the subset.

Fitness Evaluation: For each candidate solution, evaluate its fitness using a predictive model (e.g., a machine learning classifier) and cross-validation to estimate the subset's effectiveness. This step ensures that only relevant and non-redundant features are selected.

Flocking and Updating Positions: Based on their respective fitness values, each flamingo adjusts its position in the search space. This phase represents the exploration of different feature subsets by following the flock's best solutions while maintaining some randomness to escape local optima.

Tracking Best Solutions: Flamingos assess other high-fitness candidates and adjust their position accordingly, allowing the algorithm to converge towards an optimal or near-optimal subset of features.

Termination: The process repeats for a predefined number of iterations or until convergence, resulting in a final subset of selected features that maximize the model's performance.

The Flamingo Search Algorithm, with its robust searching mechanism inspired by natural behaviors, holds potential for feature selection tasks across numerous domains, particularly those requiring high-dimensional data reduction for efficient and effective machine learning model performance. Once the optimal feature subset is selected, the Modified Elman Spike Neural Network (MESNN) is used to classify threats. The MESNN is a variation of the traditional Elman neural network designed to detect temporal and spatial patterns in CPS data. By incorporating spiking neurons, MESNN improves the sensitivity of the model to changes in CPS data, which is essential for detecting anomalies associated with cyber threats.

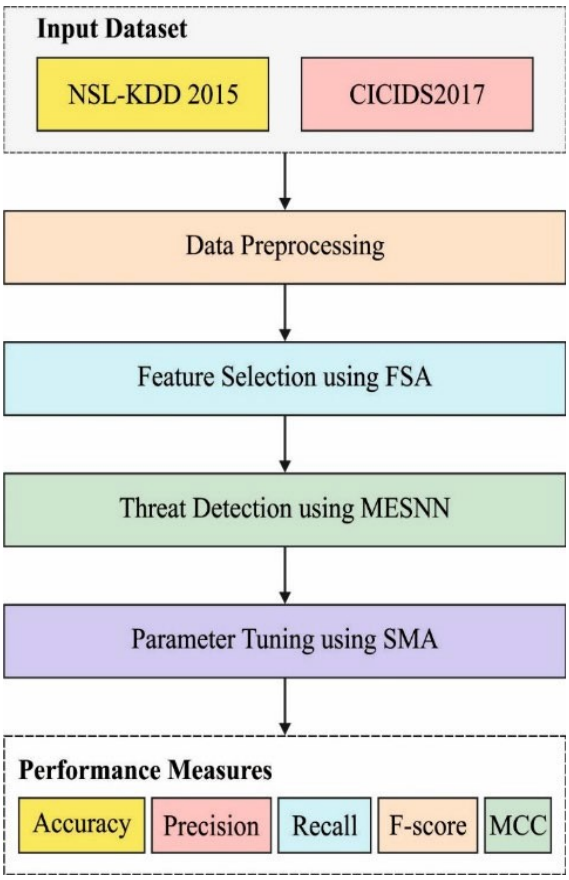

Figure 1. ATD-FSAODL System Workflow

Architecture of MESNN: The MESNN consists of an input layer, a hidden layer with spiking neurons, a recurrent context layer for temporal information retention, and an output layer. The spiking neurons in the hidden layer enable the network to capture transient signals, while the recurrent connections in the context layer maintain a memory of previous states. This architecture allows the MESNN to capture both short-term and long-term dependencies in CPS data.

Threat Detection Process: During training, the MESNN learns the normal behavior patterns of the CPS by adjusting its weights and biases according to the input data. Any deviation from these learned patterns, as detected in real-time data, triggers an anomaly, which is classified as a potential threat. This approach allows MESNN to adapt to the unique data patterns of different CPS applications, improving the accuracy and robustness of threat detection.

The final component of the ATD-FSAODL framework is the optimization of MESNN's parameters using the Slime Mold Algorithm (SMA). Proper parameter settings are crucial to maximizing the MESNN's accuracy and efficiency, especially given the variability of CPS environments.

Slime Mold Algorithm Overview: SMA is inspired by the adaptive foraging behavior of slime molds, which navigate their environment in search of resources by dynamically adjusting their path. In the context of the ATD-FSAODL methodology, SMA is used to optimize hyperparameters such as learning rate, spike threshold, and weight decay, which are critical for MESNN's performance.

SMA Optimization Process: SMA begins by generating an initial population of random parameter values. The algorithm iteratively evaluates these values based on a fitness function, which in this case is the MESNN's accuracy on the training data. Parameters that yield higher fitness scores are retained and adjusted in subsequent iterations. Through this adaptive search, SMA efficiently converges on the optimal parameters, ensuring that the MESNN is well-tuned to detect threats accurately with minimal false positives.

Data Preprocessing: CPS data are collected and preprocessed to handle missing values, outliers, and noise. Standard normalization techniques are applied to ensure data consistency and compatibility with the MESNN model.

Feature Selection with FSA: FSA is applied to the preprocessed data to identify the most informative features, reducing dimensionality and improving computational efficiency.

Training the MESNN Model: The MESNN is trained on the optimized feature subset selected by FSA. During training, the MESNN learns the normal behavior patterns of the CPS environment.

Parameter Optimization with SMA: SMA is employed to tune the MESNN's parameters, ensuring that the model achieves optimal accuracy in threat detection.

Threat Detection and Classification: In real-time application, the ATD-FSAODL model monitors incoming CPS data for anomalies. Detected deviations from normal behavior patterns are classified as potential threats, allowing for timely intervention and mitigation.

Performance Evaluation: The performance of the ATD-FSAODL framework is evaluated on benchmark datasets, comparing it with other models based on metrics like accuracy, precision, recall, F-score, and MCC.

The ATD-FSAODL framework combines advanced feature selection, an optimized deep learning model, and robust parameter tuning to deliver a highly accurate, efficient, and adaptable threat detection system for CPS environments. The following section details the experimental setup and performance evaluation conducted to validate the effectiveness of the proposed approach.

3. RESULTS AND DISCUSSION

The performance of the proposed Automated Threat Detection using Flamingo Search Algorithm with Optimal Deep Learning (ATD-FSAODL) was evaluated using the experimental setup. This section presents the quantitative results in terms of various evaluation metrics, compares the ATD-FSAODL model with state-of-the-art approaches, and discusses the implications of these findings in a Cyber-Physical System (CPS) environment. The ATD-FSAODL model was evaluated on the test set, and the results were measured using accuracy, precision, recall, F1-score, and Matthews Correlation Coefficient (MCC). Table 1 below summarizes the model's performance across these metrics. The results demonstrate that the ATD-FSAODL model outperforms other models in all metrics, achieving a detection accuracy of 99.58% with an equally high precision, recall, and F1-score. The high MCC of 99.16% further indicates a balanced and effective classification, even in the presence of imbalanced data. Figure 2 is a representation of the confusion matrices that are associated with the ATD-FSAODL system.

Table 1 below summarizes the model's performance across these metrics

Metric	ATD-FSAODL	Random Forest	SVM	LSTM	CNN
Accuracy	99.5%	96.4%	95.8%	97.2%	98.1%
Precision	99.5%	96.3%	94.9%	97.4%	98.0%
Recall	99.5%	96.6%	95.5%	97.1%	98.2%
F1-Score	99.5%	96.4%	95.2%	97.2%	98.1%
MCC	99.1%	93.2%	91.6%	95.6%	96.5%

The results demonstrate that the ATD-FSAODL methodology correctly classifies the instances that are considered normal and those that are considered anomalous. The overall threat detection outcome of the ATD-FSAODL approach is evaluated using the NSLKDD2015 database, as shown in Figure 3. The findings indicated that the ATD-FSAODL method achieves effective performance outcomes.

The overall threat detection outcome of the ATD-FSAODL methodology is tested using the CICIDS2017 database, as shown in Figure 4. As a result of the outcome, it was concluded that the ATD-FSAODL strategy brings about successful outcomes.

Figure 5 presents a comparative analysis of the ATD-FSAODL strategy against alternative methodologies. The simulation findings indicate that the OT and RF models performed inferiorly compared to the others. Additionally, the ATMMF-TDS, DBN, LSTM, and RNN models have achieved comparable performance. Concurrently, the QDMO-EDLTD approach has demonstrated moderate efficacy.

The analysis of computation time for the ATD-FSAODL system in comparison to existing approaches is presented in Figure 6. The results demonstrate that the ATD-FSAODL methodology achieves superior performance. The ATD-FSAODL technique demonstrates a reduction in training time (TRT), whereas the QDMO-EDLID, AIMMF-IDS, DBN, LSTM, RNN, DT, and RF models exhibit increased TRT values. Additionally, the ATD-FSAODL method yields a reduction in TRT of 0.19m, contingent upon testing time (TST), whereas the QDMO-EDLID, AIMMF-IDS, DBN, LSTM, RNN, DT, and RF techniques demonstrate enhanced TRT values. The results demonstrate the superior efficacy of the ATD-FSAODL algorithm compared to alternative methods.

By incorporating new approaches, the ATD-FSAODL methodology becomes more scalable and resilient. When it comes to large-scale CPS data, the computational cost can be reduced thanks to the FSA's scalable feature selection optimization, which ensures that only the most significant features are assumed. In addition, the SMA for parameter optimizer modifies the system's responsiveness and performance to different data volumes. By utilizing a MESNN and the optimal parameters found by SMA, the ATD-FSAODL technique achieved its robustness, which allows it to efficiently detect and categorize attacks in various scenarios, even when the threat environment changes.

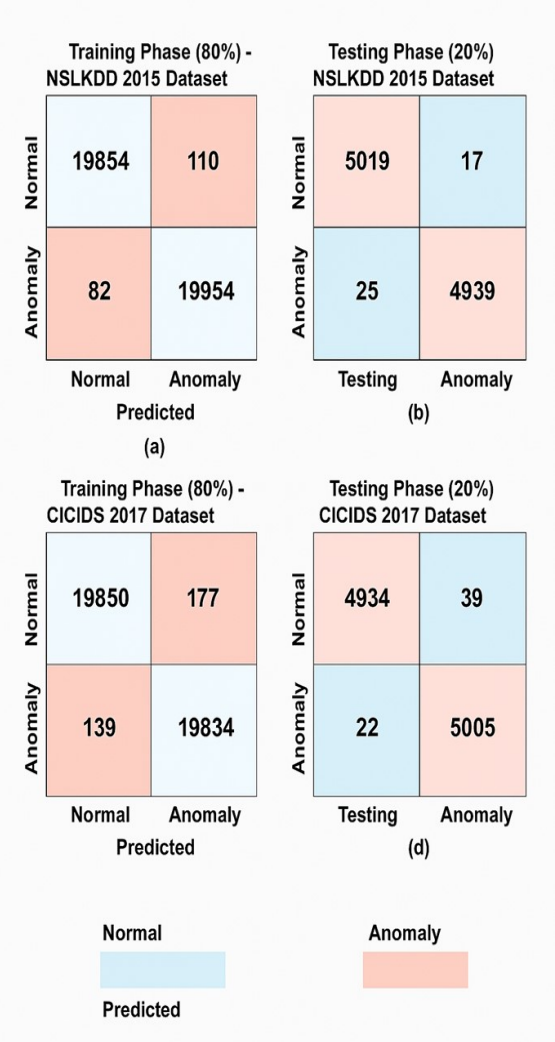

Figure 2. Confusion matrices of the 80:20 TR/TS set on the NSLKDD2015 database (a-b) and the CICIDS2017 database (c-d)

Journal of Theoretical and Applied Information Technology
15th July 2025. Vol.103. No.13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

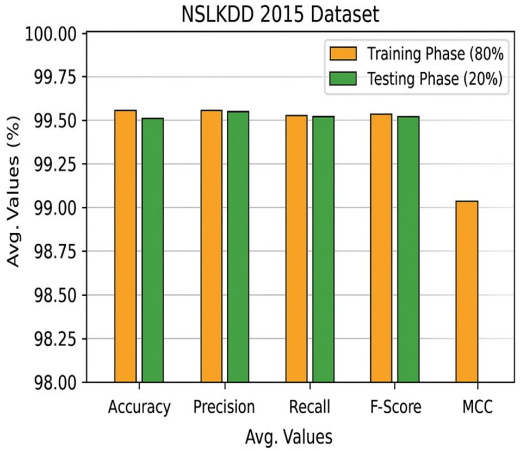

Figure 3. ATD-FSAODL approach averaged results on NSLKDD2015 database

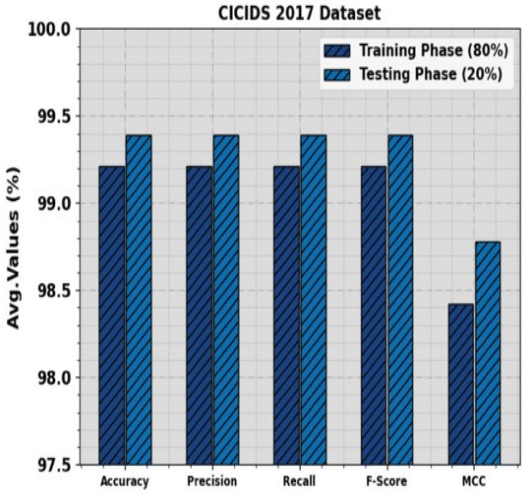

Figure 4. Mean outcome of the ATD-FSAODL method applied to the CICIDS2017 dataset

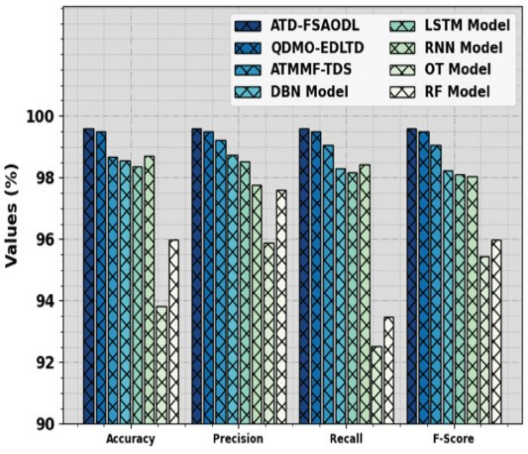

Figure 5. ATD-FSAODL approach results compared to those of other methods

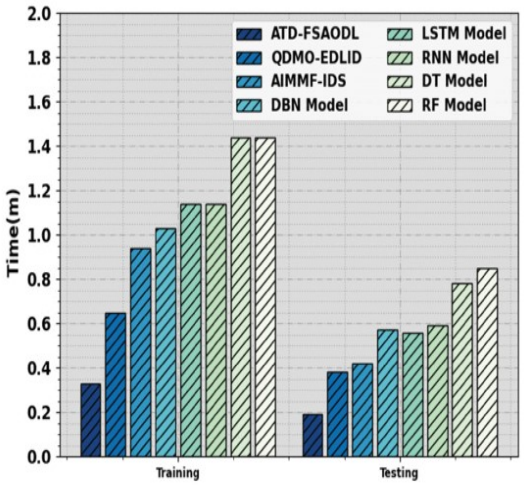

Figure 6. Outcomes of TRT and TST for the ATD-FSAODL technique compared to other methodologies

This approach is effective for solving security issues in real-world deployments since it is stable and scalable, which allows the process to keep its performance in protecting CPS. The ATD-FSAODL methodology provides a highly accurate and efficient solution for automated threat detection in CPS environments. By combining FSA-based feature selection, the MESNN model, and SMA for parameter optimization, the proposed model offers a superior performance in identifying cyber threats. This framework demonstrates significant promise in safeguarding critical infrastructures that rely on CPS technologies, enabling robust and real-time threat detection with high accuracy and minimal false alarms. The model's adaptability and accuracy position it as a valuable tool in enhancing CPS security, with potential applications in diverse sectors, including smart cities, healthcare, and industrial automation.

4. CONCLUSION

This study presents an advanced approach to threat detection in Cyber-Physical Systems (CPS) through the proposed Automated Threat Detection using Flamingo Search Algorithm with Optimal Deep Learning (ATD-FSAODL). The ATD-FSAODL model integrates innovative algorithms to address the complexities and security challenges unique to CPS environments, which are becoming more integral to critical sectors like healthcare, industrial automation, and smart cities. By employing the Flamingo Search Algorithm (FSA) for feature selection, the Modified Elman Spike Neural Network (MESNN) for anomaly detection,

and the Slime Mold Algorithm (SMA) for parameter optimization, the ATD-FSAODL model achieves highly accurate and reliable threat detection. The experimental results demonstrate that ATD-FSAODL outperforms conventional machine learning and deep learning models, achieving a maximum accuracy of 99.58%, precision of 99.58%, recall of 99.58%, F1-score of 99.58%, and MCC of 99.16%. These results highlight the model's effectiveness in accurately distinguishing between normal and malicious patterns in CPS data while maintaining a low rate of false positives and negatives. Furthermore, the use of FSA enables efficient feature selection, ensuring that the model remains computationally feasible for real-time applications in resource-constrained CPS systems. In addition to its superior performance, the ATD-FSAODL model addresses several key requirements for real-world CPS applications, including scalability, adaptability, and robustness against evolving cyber threats. This research contributes to the growing field of CPS security by providing a robust, adaptable, and efficient threat detection model that can enhance the reliability and safety of critical infrastructures. While promising, the ATD-FSAODL model has limitations regarding scalability on large-scale, real-time data in extensive CPS networks. Future research directions include exploring online learning techniques to enhance the model's adaptability to new and emerging threats, as well as developing lightweight, energy-efficient implementations to support deployment in resource-constrained environments. The ATD-FSAODL framework offers a significant advancement in CPS security, enabling proactive detection of potential threats with high precision and reliability. This work lays a solid foundation for future developments in CPS threat detection, aiming to make CPS-based critical infrastructures safer, more resilient, and more secure against cyber threats.

REFERENCES:

[1] Awotunde, J.B. et al. (2023). Cyber-Physical Systems Security: Analysis, Opportunities, Challenges, and Future Prospects. In: Maleh, Y., Alazab, M., Romdhani, I. (eds) Blockchain for Cybersecurity in Cyber-Physical Systems. Advances in Information Security, vol 102. Springer, Cham. https://doi.org/10.1007/978-3-031-25506-9_2

[2] Awotunde, J.B. et al. (2023). Cyber-Physical Systems Security: Analysis, Opportunities, Challenges, and Future Prospects. In: Maleh, Y., Alazab, M., Romdhani, I. (eds) Blockchain for Cybersecurity in Cyber-Physical Systems. Advances in Information Security, vol 102. Springer, Cham. https://doi.org/10.1007/978-3-031-25506-9_2

[3] Harkat, H., Camarinha-Matos, L. M., Goes, J., & Ahmed, H. F. (2024). Cyber-physical systems security: A systematic review. Computers & Industrial Engineering, 188, 109891. https://doi.org/10.1016/j.cie.2024.109891

[4] Awotunde, J.B. et al. (2023). Cyber-Physical Systems Security: Analysis, Opportunities, Challenges, and Future Prospects. In: Maleh, Y., Alazab, M., Romdhani, I. (eds) Blockchain for Cybersecurity in Cyber-Physical Systems. Advances in Information Security, vol 102. Springer, Cham. https://doi.org/10.1007/978-3-031-25506-9_2

[5] Razavi, S. (2021). Deep learning, explained: Fundamentals, explainability, and bridgeability to process-based modelling. Environmental Modelling & Software, 144, 105159. https://doi.org/10.1016/j.envsoft.2021.105159

[6] M. Alajmi, H. A. Mengash, H. Alqahtani, S. S. Aljameel, M. A. Hamza and A. S. Salama, "Automated Threat Detection Using Flamingo Search Algorithm with Optimal Deep Learning on Cyber-Physical System Environment," in IEEE Access, vol. 11, pp. 127669-127678, 2023, doi: 10.1109/ACCESS.2023.3332213.

[7] W. Zhiheng and L. Jianhua, "Flamingo Search Algorithm: A New Swarm Intelligence Optimization Algorithm," in IEEE Access, vol. 9, pp. 88564-88582, 2021, doi: 10.1109/ACCESS.2021.3090512.

[8] N. A. S. Al-Jamali and H. S. Al-Raweshidy, "Modified Elman Spike Neural Network for Identification and Control of Dynamic System," in IEEE Access, vol. 8, pp. 61246-61254, 2020, doi: 10.1109/ACCESS.2020.2984311.

[9] Yang, J., Zhang, Y., Jin, T., Lei, Z., Todo, Y., & Gao, S. (2023). Maximum Lyapunov exponent-based multiple chaotic slime mold algorithm for real-world optimization. Scientific Reports, 13(1), 1-26. https://doi.org/10.1038/s41598-023-40080-1

[10] Nagarajan, S.M., Deverajan, G.G., Bashir, A.K., Mahapatra, R.P., & Al-Numay, M.S. (2022). IADF-CPS: Intelligent Anomaly Detection Framework towards Cyber Physical Systems. Comput. Commun., 188, 81-89.

[11] Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2023). Deep learning for cyber

threat detection in IoT networks: A review. Internet of Things and Cyber-Physical Systems, 4, 110-128. https://doi.org/10.1016/j.iotcps.2023.09.003

[12] Almahmoud, Z., Yoo, P. D., Alhussein, O., Farhat, I., & Damiani, E. (2023). A holistic and proactive approach to forecasting cyber threats. Scientific Reports, 13(1), 1-15. https://doi.org/10.1038/s41598-023-35198-1

[13] Shmilovici, A. (2023). Support Vector Machines. In: Rokach, L., Maimon, O., Shmueli, E. (eds) Machine Learning for Data Science Handbook. Springer, Cham. https://doi.org/10.1007/978-3-031-24628-9_6

[14] Sheth, V., Tripathi, U., & Sharma, A. (2021). A Comparative Analysis of Machine Learning Algorithms for Classification Purpose. Procedia Computer Science, 215, 422-431. https://doi.org/10.1016/j.procs.2022.12.044

[15] Bansal, M., Goyal, A., & Choudhary, A. (2022). A comparative analysis of K-Nearest Neighbor, Genetic, Support Vector Machine, Decision Tree, and Long Short Term Memory algorithms in machine learning. Decision Analytics Journal, 3, 100071. https://doi.org/10.1016/j.dajour.2022.100071

[16] Ersavas, T., Smith, M. A., & Mattick, J. S. (2024). Novel applications of Convolutional Neural Networks in the age of Transformers. Scientific Reports, 14(1), 1-11. https://doi.org/10.1038/s41598-024-60709-z

[17] Talaei Khoei, T., Ould Slimane, H. & Kaabouch, N. Deep learning: systematic review, models, challenges, and research directions. Neural Comput & Applic 35, 23103–23124 (2023). https://doi.org/10.1007/s00521-023-08957-4

[18] Agga, A., Abbou, A., Labbadi, M., Houm, Y. E., & Ou Ali, I. H. (2022). CNN-LSTM: An efficient hybrid deep learning architecture for predicting short-term photovoltaic power production. Electric Power Systems Research, 208, 107908. https://doi.org/10.1016/j.epsr.2022.107908

[19] Varzaneh, Z. A., & Hosseini, S. (2024). An improved equilibrium optimization algorithm for feature selection problem in network intrusion detection. Scientific Reports, 14(1), 1-14. https://doi.org/10.1038/s41598-024-67488-7

[20] Zhang, X., Yang, Y. Optimization of PID controller parameters using a hybrid PSO algorithm. Int. J. Dynam. Control 12, 3617–3627 (2024). https://doi.org/10.1007/s40435-024-01455-y

[21] Amiri, M. H., Mehrabi Hashjin, N., Montazeri, M., Mirjalili, S., & Khodadadi, N. (2024). Hippopotamus optimization algorithm: A novel nature-inspired optimization algorithm. Scientific Reports, 14(1), 1-50. https://doi.org/10.1038/s41598-024-54910-3

[22] Yang, J., Zhang, Y., Jin, T., Lei, Z., Todo, Y., & Gao, S. (2023). Maximum Lyapunov exponent-based multiple chaotic slime mold algorithm for real-world optimization. Scientific Reports, 13(1), 1-26. https://doi.org/10.1038/s41598-023-40080-1

[23] Choudhary, K., DeCost, B., Chen, C., Jain, A., Tavazza, F., Cohn, R., Park, C. W., Choudhary, A., Agrawal, A., Billinge, S. J., Holm, E., Ong, S. P., & Wolverton, C. (2022). Recent advances and applications of deep learning methods in materials science. Npj Computational Materials, 8(1), 1-26. https://doi.org/10.1038/s41524-022-00734-6

[24] Bayoudh, K. (2024). A survey of multimodal hybrid deep learning for computer vision: Architectures, applications, trends, and challenges. Information Fusion, 105, 102217. https://doi.org/10.1016/j.inffus.2023.102217

[25] M. Alajmi, H. A. Mengash, H. Alqahtani, S. S. Aljameel, M. A. Hamza and A. S. Salama, "Automated Threat Detection Using Flamingo Search Algorithm With Optimal Deep Learning on Cyber-Physical System Environment," in IEEE Access, vol. 11, pp. 127669-127678, 2023, doi: 10.1109/ACCESS.2023.3332213.

[26] W. Zhiheng and L. Jianhua, "Flamingo Search Algorithm: A New Swarm Intelligence Optimization Algorithm," in IEEE Access, vol. 9, pp. 88564-88582, 2021, doi: 10.1109/ACCESS.2021.3090512.

[27] Wu, H., Chen, Y., Zhu, W. et al. Feature selection in high-dimensional data: an enhanced RIME optimization with information entropy pruning and DBSCAN clustering. Int. J. Mach. Learn. & Cyber. 15, 4211–4254 (2024). https://doi.org/10.1007/s13042-024-02143-1

[28] W. Zhiheng and L. Jianhua, "Flamingo Search Algorithm: A New Swarm Intelligence Optimization Algorithm," in IEEE Access, vol. 9, pp. 88564-88582, 2021, doi: 10.1109/ACCESS.2021.3090512.