International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A Metaheuristic-Optimized Deep Learning Framework For Cyberattack Detection In Cyber-Physical Systems

[1]A Emmanuel Raju,[2]Nerella Harsha Vardhan,[3]Pinjari Roshan Jameel,[4]Yammani Vishal

[1]Assistant Professor, Computer Science Of Engineering, Dr K V Subba Reddy Institute of Technology

[2,3,4]B. Tech Students, Computer Science Of Engineering, Dr K V Subba Reddy Institute of Technology

ABSTRACT

Cyber-Physical Systems (CPS) integrate computational components with physical processes and are widely used in critical infrastructures such as smart grids, healthcare systems, transportation, and industrial automation. However, the increasing connectivity of these systems makes them vulnerable to various cyberattacks that can disrupt operations and cause serious damage. Traditional security mechanisms often struggle to detect sophisticated and evolving threats in real time. To address this challenge, this study proposes an optimized deep learning model for cyberattack detection in Cyber-Physical Systems using binary metaheuristic techniques. The proposed approach combines deep learning algorithms with binary metaheuristic optimization to enhance feature selection and improve detection accuracy. Binary metaheuristics are employed to identify the most relevant features from large and complex CPS datasets, reducing computational complexity while maintaining high predictive performance. The optimized feature set is then used to train a deep learning model capable of accurately distinguishing between normal system behavior and potential cyberattacks. Experimental results demonstrate that the proposed model significantly improves detection performance compared to traditional machine learning methods. The system achieves higher accuracy, better precision and recall, and reduced false positive rates. Additionally, the optimization process enhances the efficiency of the deep learning model by minimizing redundant features and improving overall system performance

Keywords: Cyber-Physical Systems (CPS), Cyberattack Detection, Deep Learning, Binary Metaheuristic Optimization, Intrusion Detection System (IDS), Feature Selection, Network Security, Artificial Intelligence, Optimization Algorithms, Machine Learning, Anomaly Detection, Internet of Things (IoT) Security, Data Classification, Intelligent Security Systems, Computational Intelligence.

I. INTRODUCTION

Cyber-Physical Systems (CPS) represent the integration of computational systems, communication networks, and physical processes. These systems are widely used in critical infrastructures such as smart grids, industrial control systems, healthcare devices, transportation systems, and smart manufacturing. In CPS environments, sensors collect data from the physical world, which is processed by computational systems to monitor and control physical operations. Although CPS improves efficiency, automation, and system reliability, the increasing connectivity of these systems exposes them to various cybersecurity threats.

With the rapid growth of the Internet of Things (IoT) and network-based communication, CPS environments have become attractive targets for cyberattacks. Attackers can exploit vulnerabilities in communication networks, sensors, or control systems to disrupt operations, manipulate data, or damage physical infrastructure. These cyberattacks can lead to severe consequences such as service disruption, financial loss, safety risks, and system failures. Therefore, detecting cyberattacks in CPS environments has become a critical research area in cybersecurity.

Traditional intrusion detection systems and rule-based security mechanisms often fail to detect sophisticated and evolving cyber threats. These conventional methods usually rely on predefined

signatures or static rules, making them ineffective against new and unknown attack patterns. To overcome these limitations, machine learning and deep learning techniques have been widely adopted for cyberattack detection. Deep learning models can automatically learn complex patterns and relationships from large datasets, enabling more accurate and efficient detection of malicious activities.

II. LITERATURE SURVEY

1. Open Set Recognition in Cybersecurity

Recent research highlights the importance of Open Set Recognition (OSR) in cybersecurity, especially for identifying unknown and zero-day attacks. Traditional classification models operate under a closed-set assumption, meaning they can only recognize attack types that were present during training. This limitation makes them ineffective against newly emerging threats. Researchers Abhijit Bendale and Terrance E. Boult introduced the concept of open space risk and proposed approaches to manage unknown classes in classification problems. Their work established a strong foundation for applying OSR techniques in intrusion detection systems, enabling better identification of unseen cyber threats.

2. Machine Learning-Based DDoS Detection

Machine learning algorithms have been widely applied for detecting Distributed Denial of Service (DDoS) attacks in modern networks. Techniques such as Support Vector Machines (SVM), Random Forest, and Artificial Neural Networks have demonstrated improved detection accuracy compared to traditional rule-based systems. These methods analyze network traffic patterns and identify abnormal behavior that indicates potential attacks. However, most machine learning models assume that all attack types are already known during training, which limits their effectiveness when encountering new or modified DDoS attack variants.

3. Deep Learning for Network Intrusion Detection

Deep learning techniques have recently gained significant attention in the field of network intrusion detection. Architectures such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks are capable of automatically learning complex traffic patterns from large datasets. CNN models effectively capture spatial features in network traffic data, while LSTM networks are useful for learning temporal dependencies in sequential traffic patterns. These capabilities allow deep learning models to achieve higher detection accuracy and improved performance. However, most existing deep learning-based intrusion detection systems still operate under closed-set assumptions and struggle to recognize previously unseen attack types.

4. Reciprocal Points Learning for Open Set Classification

Reciprocal Points Learning (RPL) has emerged as an effective technique for addressing the challenges of open set classification. This approach introduces representative reciprocal points within the feature space to create compact decision boundaries between known and unknown classes. By minimizing open space risk, RPL improves the model's ability to reject unknown samples during classification. Research in image recognition and pattern recognition domains has demonstrated that RPL significantly improves the detection of unseen classes, indicating strong potential for its application in cybersecurity and network intrusion detection systems.

5. Open Set Intrusion Detection Systems

Recent studies have explored the integration of Open Set Recognition techniques into intrusion detection systems to address the limitations of traditional models. Methods such as threshold-based rejection mechanisms, distance-based classification approaches, and generative models have been proposed to detect unknown attacks. These approaches show promising results in identifying zero-day threats and reducing false positive rates. However, many existing solutions still face challenges related to scalability,

efficiency, and accurate detection of unknown DDoS attacks. Therefore, there is a need for more advanced frameworks that combine deep learning techniques with open set recognition methods such as Reciprocal Points Learning.

III. EXISTING SYSTEM

The existing cyberattack detection systems in Cyber-Physical Systems (CPS) mainly rely on traditional intrusion detection techniques and machine learning models. These systems analyze network traffic data and system behavior to identify malicious activities such as Distributed Denial of Service (DDoS) attacks. Most existing solutions use supervised learning algorithms like Support Vector Machines (SVM), Decision Trees, and Random Forest to classify network traffic into normal or attack categories.

Traditional intrusion detection systems generally operate under a closed-set classification approach, where the model is trained only on known attack types. As a result, the system can only detect attacks that were previously seen during the training phase. When new or unknown attacks occur, these systems often fail to recognize them and may incorrectly classify them as normal traffic.

Recent approaches have incorporated deep learning techniques such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to improve detection accuracy. These models can automatically extract complex features from large datasets and identify patterns associated with cyberattacks. However, most of these deep learning-based systems still assume that all attack classes are known in advance.

IV. PROPOSED SYSTEM

The proposed system introduces an optimized deep learning framework for detecting cyberattacks in Cyber-Physical Systems (CPS). The system integrates advanced deep learning techniques with binary metaheuristic optimization to improve the detection accuracy and efficiency of cyberattack detection. Unlike traditional systems that rely on closed-set classification, the proposed approach is designed to identify both known and unknown attack patterns in network traffic.

In this system, network traffic data is first collected and preprocessed to remove noise and irrelevant information. Feature extraction is then performed to obtain important characteristics of the network traffic. To further improve the model's performance, a binary metaheuristic optimization technique is applied for feature selection. This process identifies the most relevant features from the dataset, reducing computational complexity and improving the efficiency of the detection model.

After selecting the optimal feature set, a deep learning model is trained to classify network traffic into normal behavior and potential cyberattacks. The model learns complex traffic patterns and relationships within the data, allowing it to detect malicious activities more accurately. The proposed system is capable of identifying suspicious patterns that may indicate unknown or emerging attack types.

V. SYSTEM ARCHITECTURE

The proposed system architecture for "Optimized Deep Learning Model for Cyberattack Detection in Cyber-Physical Systems Using Binary Metaheuristics" is designed to efficiently identify and classify cyberattacks in cyber-physical environments by integrating deep learning techniques with metaheuristic-based optimization. The architecture consists of multiple interconnected layers that handle data acquisition, preprocessing, feature optimization, deep learning–based classification, and attack detection. Each component works collaboratively to ensure accurate detection of malicious activities while maintaining the performance and reliability of the cyber-physical system.

The first component of the architecture is the data acquisition layer, which collects network and system activity data from cyber-physical systems such as industrial control systems, smart grids, Internet of Things (IoT) devices, and sensor networks. These

systems continuously generate large volumes of heterogeneous data including packet-level network traffic, device logs, sensor readings, and control signals. The collected data may come from publicly available cybersecurity datasets or real-time monitoring systems deployed in CPS environments. This layer ensures that the system has access to diverse and representative data required for training and evaluating the cyberattack detection model.

After data collection, the system moves to the data preprocessing and feature extraction layer, where raw data is cleaned and transformed into a structured format suitable for machine learning models. In this stage, missing values, noise, and redundant information are removed to improve data quality. Feature extraction techniques are applied to identify important attributes such as traffic patterns, packet size, protocol types, and communication frequency. Normalization and encoding methods are also used to convert categorical and numerical attributes into standardized forms. This preprocessing stage helps reduce data complexity and prepares the dataset for efficient learning by the deep learning model.

The next stage in the architecture is the binary metaheuristic optimization module, which performs intelligent feature selection to improve detection accuracy and reduce computational overhead. Binary metaheuristic algorithms such as Binary Particle Swarm Optimization, Binary Genetic Algorithm, or Binary Grey Wolf Optimization are employed to search for the optimal subset of features from the extracted dataset. These algorithms evaluate different feature combinations and iteratively update candidate solutions to identify the most informative features that contribute significantly to cyberattack detection. By eliminating irrelevant or redundant attributes, the optimization module enhances the performance and efficiency of the deep learning classifier.

Following feature optimization, the refined dataset is passed to the deep learning detection module, which is responsible for identifying and classifying cyberattacks. This module uses a deep neural network architecture capable of learning complex patterns and relationships within the optimized feature set. The deep learning model is trained on labeled datasets containing both normal and malicious traffic samples. During training, the network automatically learns hierarchical representations of attack patterns and system behavior. Once trained, the model can accurately classify incoming data into categories such as normal activity or different types of cyberattacks.

The attack detection and decision layer processes the output generated by the deep learning model. Based on the predicted class labels and confidence scores, the system determines whether the observed activity represents a potential cyber threat. Feedback from detection results is used to retrain and improve the deep learning model, ensuring that the system remains effective against evolving cyber threats. If malicious behavior is detected, the system generates alerts and provides information about the type and severity of the attack. This layer enables real-time monitoring and rapid response, allowing administrators to take preventive or corrective actions to protect the cyber-physical infrastructure.

Finally, the architecture includes a monitoring and feedback module, which continuously evaluates the performance of the detection system and updates the model when new data or attack patterns emerge. Feedback from detection results is used to retrain and improve the deep learning model, ensuring that the system remains effective against evolving cyber threats. This adaptive capability is essential for maintaining long-term security in dynamic cyber-physical environments where new vulnerabilities and attack strategies frequently arise.

Overall, the proposed system architecture integrates data processing, optimization, and deep learning techniques into a unified framework for intelligent cyberattack detection in cyber-physical systems. Feedback from detection results is used to retrain and improve the deep learning model, ensuring that the system remains effective against evolving cyber threats. By combining binary metaheuristic feature selection with deep learning classification, the system achieves improved detection accuracy, reduced computational complexity, and enhanced robustness against sophisticated cyber threats.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

Fig 5.1: Structure of the Proposed System

VI. IMPLEMENTATION

Fig 6.1: Home Page

Fig 6.2: Profile Details

Fig 6.3: Admin Dashboard

Fig 6.4: Prediction Page

Fig 6.5: Result Page

VII. CONCLUSION

In this work, an optimized deep learning-based framework for cyberattack detection in Cyber-Physical Systems (CPS) has been presented. The system focuses on identifying Distributed Denial of Service (DDoS) attacks by combining advanced machine learning techniques with feature optimization methods. Traditional intrusion detection systems often operate under closed-set assumptions and are unable to effectively detect unknown or emerging attack patterns. To overcome these limitations, the proposed approach enhances detection capability by incorporating optimized feature selection and intelligent learning models.

The system processes network traffic data through preprocessing and feature extraction stages, followed by binary metaheuristic optimization to select the most relevant features. These optimized features are

then used to train a deep learning model capable of accurately classifying network behavior. By reducing redundant data and focusing on significant traffic characteristics, the model achieves improved detection accuracy and reduced computational complexity.

The results demonstrate that the proposed system is capable of detecting both known and suspicious attack patterns with better efficiency compared to traditional approaches. It also reduces false alarm rates and improves the overall reliability of network security monitoring. This makes the system suitable for real-time applications in Cyber-Physical Systems where network reliability and security are critical.

VIII. FUTURE SCOPE

Although the proposed cyberattack detection system provides improved performance in identifying DDoS attacks, there are several areas where the system can be further enhanced. Future research can focus on improving the model's adaptability, scalability, and detection capabilities in complex network environments.

One possible improvement is the integration of advanced deep learning architectures such as hybrid models that combine Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. These hybrid models can capture both spatial and temporal patterns in network traffic data, leading to more accurate detection of sophisticated cyberattacks.

Another future enhancement is the incorporation of real-time threat intelligence and adaptive learning mechanisms. This would allow the system to continuously learn from new attack patterns and update the model automatically without requiring manual retraining. Such an approach would improve the system's ability to detect emerging and zero-day attacks.

Future work can also focus on expanding the dataset used for training and testing the model. Using larger and more diverse datasets will improve the generalization capability of the system and make it more effective in real-world network environments.

IX. REFERENCES

[1] J. Zhang, L. Pan, Q. L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 377–402, 2022.
https://doi.org/10.1109/JAS.2021.1004261

[2] R. Mitchell and I. R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, 2014.
https://doi.org/10.1145/2542049

[3] S. Soliman, M. A. A. Alazab, and A. A. A. El-Latif, "Deep learning-based intrusion detection approach for securing industrial IoT," *Alexandria Engineering Journal*, vol. 72, pp. 475–486, 2023.
https://doi.org/10.1016/j.aej.2023.04.020

[4] M. Catillo, A. Carcano, and M. Ficco, "CPS-GUARD: Intrusion detection for cyber-physical systems using autoencoders," *Computers & Security*, vol. 124, 2023.
https://doi.org/10.1016/j.cose.2023.102964

[5] M. Umer, M. Sher, and Y. Bi, "Deep learning-based intrusion detection methods in cyber-physical systems," *Electronics*, vol. 11, no. 20, 2022.
https://doi.org/10.3390/electronics11203326

[6] S. S. Abosuliman and M. H. Alshammari, "Deep learning techniques for securing cyber-physical systems in Industry 4.0 environments," *Computers & Electrical Engineering*, vol. 105, 2023.
https://doi.org/10.1016/j.compeleceng.2023.108494

[7] S. Thakur and R. Jain, "Intrusion detection in cyber-physical systems using deep learning techniques," *Computers & Electrical Engineering*, vol. 91, 2021.
https://doi.org/10.1016/j.compeleceng.2021.107043

[8] V. F. Santos, J. Barros, and M. Vieira, "Assessing machine learning techniques for intrusion detection in cyber-physical systems," *Energies*, vol. 16, no. 16, 2023.
https://doi.org/10.3390/en16166058

[9] M. M. Asiri et al., "Hybrid metaheuristics feature selection with stacked deep learning-enabled cyber-attack detection model," *Computer Systems Science and Engineering*, vol. 45, no. 2, pp. 1679–1694, 2023.
https://doi.org/10.32604/csse.2023.031063

[10] A. T. Azar et al., "Enhanced metaheuristics with hierarchical deep learning-based attack detection for cloud cyber-physical systems," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, 2024.
https://doi.org/10.48084/etasr.8286

[11] S. S. Kareem et al., "An effective feature selection model using hybrid metaheuristics for cyber-attack detection," *Computational Intelligence and Neuroscience*, 2022. https://doi.org/10.1155/2022/8962996

[12] A. Hozouri, A. Mirzaei, and M. Effatparvar, "A comprehensive survey on intrusion detection systems with advances in machine learning and deep learning," *Discover Artificial Intelligence*, vol. 5, 2025. https://doi.org/10.1007/s44163-025-00578-1

[13] S. E. Quincozes et al., "An extended assessment of metaheuristics-based feature selection for intrusion detection systems," *Annals of Telecommunications*, vol. 77, pp. 457–471, 2022. https://doi.org/10.1007/s12243-022-00864-5

[14] A. Daniel and P. Ravi, "Optimal feature selection with graph convolutional network for malware detection in cyber-physical systems," *Computers & Electrical Engineering*, vol. 104, 2023. https://doi.org/10.1016/j.compeleceng.2022.108416

[15] S. Rehman et al., "Intrusion detection system framework for cyber-physical environments using hybrid detection techniques," *Ain Shams Engineering Journal*, 2025. https://doi.org/10.1016/j.asej.2024.102593