International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

SecureCPS-Opt: A Hybrid Optimization and Federated AI Framework for Efficient and Privacy-Preserving Attack Detection in IoT-Enabled Cyber-Physical Systems

Mr.M.Raja Kumar[1], Pepakayala Bhavani Sri Alekhya[2], Dasari Asritha[3], Sada Uma Maheswara Rao[4], Thimmasatthi Venkateswarlu[5], Kollu Rajesh[6]
[1]Associate Professor, [2, 3,4,5,6B.tech] Students Department of CSE ,
Pragati Engineering College, Surampalem , Andhra Pradesh, India

Abstract- The rapid growth of Internet of Things (IoT) devices has significantly improved automation, connectivity, and data-driven decision-making across various domains such as healthcare, smart cities, agriculture, and industrial systems. However, the increasing number of interconnected devices has also introduced serious security challenges. IoT-enabled cyber-physical systems are highly vulnerable to cyber-attacks such as Distributed Denial of Service (DDoS), data injection, botnet attacks, and unauthorized access. Traditional machine learning techniques often struggle to provide high detection accuracy due to imbalanced datasets, high-dimensional features, and inefficient parameter tuning. In this project, a hybrid deep learning-based intrusion detection framework is proposed for identifying security attacks in IoT-enabled cyber-physical systems. The proposed model combines Convolutional Neural Network (CNN) and Deep Belief Network (DBN) to improve feature learning and classification performance. To enhance the model's efficiency and convergence speed, a novel hybrid optimization technique called Seagull Adopted Elephant Herding Optimization (SAEHO) is employed for tuning the classifier weights. The proposed framework is evaluated using standard IoT intrusion detection datasets such as UNSW-NB15 and BoT-IoT. Performance is measured using metrics including accuracy, precision, sensitivity, specificity, False Positive Rate (FPR), False Negative Rate (FNR), and Matthews Correlation Coefficient (MCC). Experimental results demonstrate that the hybrid classifier optimized using SAEHO outperforms conventional machine learning and optimization-based models in terms of detection accuracy and reduced error rates. The developed system provides an effective and scalable solution for enhancing security in IoT-enabled cyber-physical environments.

Keywords – Internet of Things (IoT), Cyber-Physical Systems (CPS), Intrusion Detection System (IDS), Deep Learning, Convolutional Neural Network (CNN), Deep Belief Network (DBN), Hybrid Optimization Algorithm, Seagull Adopted Elephant Herding Optimization (SAEHO), Cyber Security, Network Attack Detection, UNSW-NB15 Dataset, BoT-IoT Dataset, Machine Learning, Performance Evaluation Metrics.

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has significantly transformed modern digital infrastructure by enabling the interconnection of billions of smart devices across diverse domains such as healthcare, smart cities, industrial automation, agriculture, and transportation. IoT-enabled cyber-physical systems (CPS) integrate sensing, computation, and communication technologies to monitor and control physical environments in real time. Although these interconnected systems enhance efficiency, automation, and productivity, they also introduce serious security vulnerabilities due to the continuous exchange of sensitive information across networks [3], [5].

Cyber-attacks targeting IoT environments have increased considerably in recent years. Common threats include Distributed Denial of Service (DDoS) attacks, data injection attacks, malware propagation, botnet activities, and unauthorized access attempts. Attackers often exploit poorly protected IoT devices to launch large-scale attacks that disrupt network services and compromise data integrity. Due to the limited computational capabilities and memory constraints of many IoT devices, implementing complex built-in security

mechanisms becomes challenging. Consequently, intrusion detection systems (IDS) play a crucial role in identifying malicious activities and protecting cyber-physical infrastructures [2], [9], [10].

Intrusion detection in IoT networks can generally be formulated as a binary classification problem, where network traffic is categorized as either normal (benign) or malicious (attack). However, detecting cyber-attacks in IoT systems remains a challenging task due to the presence of high-dimensional traffic data, imbalanced datasets, evolving attack patterns, and large-scale network traffic volumes. Manual analysis of such large datasets is impractical and inefficient. Therefore, machine learning (ML) and deep learning (DL) techniques have become increasingly important for automating intrusion detection and improving detection accuracy [6], [13], [14].

Traditional machine learning approaches such as Support Vector Machines (SVM), Decision Trees, Random Forests, and Artificial Neural Networks have been widely applied to intrusion detection problems. These methods can effectively learn patterns from network traffic data and classify suspicious activities. However, conventional ML models may suffer from limitations such as suboptimal parameter tuning, slow convergence, and higher false positive rates when dealing with complex IoT traffic patterns [10], [14].

To overcome these limitations, deep learning models such as Convolutional Neural Networks (CNN) and Deep Belief Networks (DBN) have been introduced for intrusion detection tasks. These models provide improved feature extraction capabilities and can capture complex nonlinear relationships within network traffic data. Nevertheless, deep learning models often require efficient optimization strategies to achieve optimal performance. Without appropriate parameter optimization, these models may lead to overfitting, increased computational complexity, and reduced generalization capability [7], [8], [11].

In this study, a hybrid deep learning–based framework is proposed for detecting cyber-attacks in IoT-enabled cyber-physical systems. The proposed model combines the feature extraction capability of CNN with the learning efficiency of DBN to improve classification performance. In addition, a hybrid optimization technique known as Seagull Adopted Elephant Herding Optimization (SAEHO) is incorporated to optimize the classifier weights and enhance model convergence. Hybrid optimization approaches have shown promising results in improving intrusion detection performance and reducing computational errors in complex cybersecurity environments [1], [4].

The effectiveness of the proposed framework is evaluated using publicly available IoT intrusion detection datasets, including UNSW-NB15 and BoT-IoT. To address dataset imbalance and evaluate model performance comprehensively, several evaluation metrics are considered, including accuracy, precision, recall, F1-score, specificity, False Positive Rate (FPR), False Negative Rate (FNR), and Matthews Correlation Coefficient (MCC). Experimental results demonstrate that the proposed Hybrid CNN-DBN classifier with SAEHO optimization achieves improved detection accuracy and reduced computational error compared with conventional machine learning approaches.

The remainder of this paper is organized as follows. Section II presents a review of related work on IoT intrusion detection and optimization techniques. Section III describes the system analysis, including existing and proposed models. Section IV explains the system architecture and design methodology. Section V outlines the implementation modules and experimental setup. Section VI discusses the results and performance evaluation. Finally, Section VII concludes the paper and highlights potential directions for future research.

II. LITERATURE SURVEY

With the rapid advancement of Internet of Things (IoT) technology, researchers have increasingly focused on developing effective security mechanisms to protect IoT-enabled cyber-physical systems from cyber-attacks. The growing number of connected devices and the continuous exchange of sensitive data across networks have significantly increased the vulnerability of IoT environments to various cyber threats. Consequently, numerous machine learning and deep learning approaches have been proposed to detect malicious activities within network traffic and improve the reliability of intrusion detection systems [3], [5].

Early studies primarily utilized traditional machine learning algorithms such as Support Vector Machines (SVM), Decision Trees, Random Forest, and K-Nearest Neighbors (KNN) for intrusion detection tasks. These techniques were capable of identifying known attack patterns with reasonable accuracy. However, they often faced challenges when applied to large-scale IoT datasets characterized by high-dimensional features and imbalanced data distributions. As a result, their detection performance tends to degrade when encountering complex or previously unseen attack patterns [10], [14].

To address these limitations, researchers began exploring deep learning techniques due to their ability to automatically extract meaningful features from raw network traffic data. Among these approaches, Convolutional Neural Networks (CNN) have gained significant attention because of their strong feature extraction capabilities and ability to capture complex patterns in large datasets. Similarly, Deep Belief Networks (DBN) have demonstrated effectiveness in identifying hidden relationships within high-dimensional data,

thereby improving intrusion detection accuracy [7], [11]. Despite their advantages, deep learning models require careful parameter tuning to achieve optimal performance. Without appropriate optimization strategies, these models may experience slow convergence, increased computational cost, and overfitting issues.

To improve the performance of deep learning–based intrusion detection systems, several optimizationalgorithms have been proposed to fine-tune model parameters. Metaheuristic optimization techniques such as the Whale Optimization Algorithm (WOA), Grey Wolf Optimization (GWO), and Sea Lion Optimization (SLnO) have been employed to enhance model convergence and reduce classification errors. These optimization strategies have shown promising results in improving detection performance in cybersecurity applications [1], [8]. However, their effectiveness may still be limited in highly dynamic IoT environments where attack patterns continuously evolve.

In addition, several researchers have proposed hybrid intrusion detection models that combine multiple machine learning or deep learning classifiers to improve detection capability. Hybrid frameworks aim to leverage the strengths of different algorithms while minimizing their individual limitations. Such approaches have demonstrated improved performance in detecting complex cyber-attacks and enhancing system robustness in IoT ecosystems [2], [4], [13]. Nevertheless, there remains a need for more efficient optimization techniques capable of improving classification accuracy while reducing false positive rates.

Based on the analysis of existing studies, it is evident that integrating deep learning models with advanced hybrid optimization strategies can significantly enhance intrusion detection performance in IoT-enabled cyber-physical systems. Therefore, this study proposes a hybrid deep learning framework integrated with a novel optimization technique to achieve improved detection accuracy, faster convergence, and enhanced stability in detecting cyber-attacks within IoT environments.

III.SYSTEM ANALYSIS

Existing System

Existing intrusion detection systems for IoT-enabled cyber-physical systems mainly rely on traditional machine learning and deep learning techniques. Researchers evaluate IoT security datasets using conventional algorithms such as Support Vector Machines (SVM), Decision Trees, Random Forest, K-Nearest Neighbors (KNN), Naïve Bayes, and Artificial Neural Networks (ANN). These models classify network traffic as either normal or malicious based on patterns learned from historical data [10], [14].

In addition to single classifiers, some studies propose hybrid approaches that combine multiple algorithms to improve detection performance. Ensemble techniques such as boosting, bagging, and majority voting are used to enhance accuracy and reduce classification errors. Deep learning models like Convolutional Neural Networks (CNN) and Deep Belief Networks (DBN) are also introduced to automatically extract complex features from network traffic data [7], [11].

To improve model performance, researchers apply optimization algorithms such as the Whale Optimization Algorithm (WOA), Grey Wolf Optimization (GWO), and other nature-inspired techniques to tune model parameters. These optimization methods aim to improve convergence speed and classification accuracy [1], [8].

Experiments are usually conducted on publicly available IoT intrusion detection datasets to evaluate the effectiveness of these approaches [3], [9]. Although existing systems provide acceptable detection results, they still face several practical limitations when applied to real-world IoT environments.

Disadvantages Of The Existing System

- **Interpretability**
  Complex deep learning models are often difficult to interpret. Understanding how a model makes decisions is important in cybersecurity applications to build trust and ensure transparency [6].

- **Overfitting and Underfitting**
  Some models may overfit the training dataset and fail to generalize to new attacks. On the other hand, underfitting can occur when the model fails to capture important patterns in the data [10], [14].

- **Imbalanced Data Handling**
  IoT intrusion datasets are usually imbalanced, where normal traffic is much higher than attack traffic. Many existing models struggle to handle this imbalance effectively [3], [9].

- **Computational Complexity**
  Deep learning and optimization-based models may require high computational power and memory. This can be challenging in large-scale IoT environments [7], [8].

- **Slow Convergence**
  Certain optimization algorithms take longer to converge, which increases training time and reduces system efficiency [1].

- **False Positive Rate**
  High false positive rates can lead to unnecessary alerts, reducing the reliability of the intrusion detection system [13].

- **Scalability Issues**
  As IoT networks grow rapidly, intrusion detection systems must handle massive volumes of data. Some existing systems fail to scale efficiently with increasing network traffic [2], [4].

- **Vulnerability to Advanced Attacks**

Attackers continuously develop new techniques to bypass detection systems. Some traditional models may fail to detect newly emerging or sophisticated attacks [5].

Proposed System

In the proposed intrusion detection framework, the IoT security dataset is first pre-processed to remove irrelevant features and normalize the data. Proper preprocessing helps improve data quality and enhances the learning capability of machine learning models [3], [9]. The dataset is then divided into training and testing sets to evaluate the performance of the proposed model.

A hybrid deep learning architecture combining Convolutional Neural Network (CNN) and Deep Belief Network (DBN) is employed for effective feature extraction and classification. CNN is utilized to extract important patterns from network traffic data, while DBN is used to learn hidden representations and improve classification accuracy [7], [11].

To further enhance model performance, a hybrid optimization algorithm known as Seagull Adopted Elephant Herding Optimization (SAEHO) is applied to optimize the weights and parameters of the classifier. Optimization techniques help improve convergence speed and reduce classification errors in intrusion detection systems [1], [8].

The proposed system is evaluated using cross-validation techniques to ensure reliable performance on imbalanced datasets. Multiple evaluation metrics are used to measure the effectiveness of the model, including accuracy, precision, recall, F1-score, False Positive Rate (FPR), False Negative Rate (FNR), Matthews Correlation Coefficient (MCC), and Area Under the Curve (AUC).

By integrating deep learning with an efficient hybrid optimization strategy, the proposed system aims to achieve higher detection accuracy, faster convergence, and improved scalability compared to existing intrusion detection approaches [2], [4], [10].

IV.SYSTEM DESIGN

System Architecture

Below diagram depicts the whole system architecture.

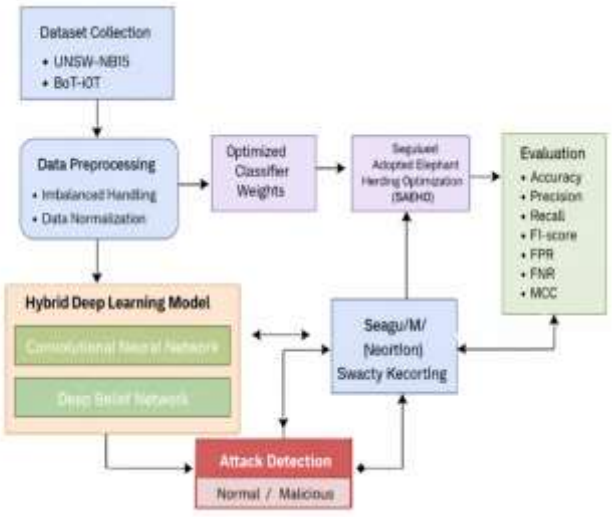

Fig. 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

Modules

Data Collection and Preprocessing

In this module, relevant IoT intrusion detection datasets such as UNSW-NB15 and BoT-IoT are collected. These datasets contain both normal network traffic and various types of cyber-attacks. The preprocessing stage includes handling missing values, removing irrelevant or redundant features, and normalizing the data to ensure uniformity. Since IoT datasets are often imbalanced, suitable techniques such as resampling are applied to reduce the impact of class imbalance and improve model performance [3], [9].

Feature Selection and Engineering

This module focuses on identifying the most important features that contribute to detecting malicious network behaviour. The dataset is carefully analysed to remove unnecessary attributes and retain meaningful ones. In some cases, new features may be derived from existing attributes to enhance the model's ability to capture hidden patterns associated with cyber-attacks. Effective feature selection helps reduce computational complexity and improves classification accuracy [10], [14].

Hybrid Deep Learning Model Training

In this stage, the pre-processed dataset is used to train the proposed hybrid deep learning model. The architecture combines Convolutional Neural Network (CNN) for efficient

feature extraction and Deep Belief Network (DBN) for accurate classification. The model learns patterns from both normal and malicious traffic data to distinguish between them effectively. Training is performed using the training dataset, while validation techniques are applied to prevent overfitting [7], [11].

Optimization Using SAEHO

To enhance the performance of the hybrid model, the Seagull Adopted Elephant Herding Optimization (SAEHO) algorithm is applied. This optimization technique is used to tune the classifier's weights and improve convergence speed. By optimizing the model parameters, the system achieves better detection accuracy and reduced error rates compared to traditional optimization methods [1], [8].

Attack Detection and Real-Time Classification

Once the model is trained and optimized, it is used to classify incoming network traffic as either normal or malicious. This module enables efficient and timely detection of cyber-attacks in IoT environments. The system can be integrated into real-time monitoring frameworks to support early attack detection and prevention [2], [4].

Model Evaluation and Continuous Monitoring

The performance of the trained model is evaluated using metrics such as accuracy, precision, recall, F1-score, False Positive Rate (FPR), False Negative Rate (FNR), and Matthews Correlation Coefficient (MCC). Continuous monitoring mechanisms can be implemented to assess the model's effectiveness over time. This allows necessary updates and improvements when new attack patterns emerge in IoT networks [6], [13].

VI .RESULTS AND DISCUSSION

To evaluate the effectiveness of the proposed intrusion detection framework, experiments were conducted using publicly available IoT datasets such as UNSW-NB15 and BoT-IoT. The dataset was divided into training and testing subsets, and cross-validation techniques were applied to ensure reliable performance evaluation. The proposed hybrid deep learning model combining Convolutional Neural Network (CNN) and Deep Belief Network (DBN) was optimized using the Seagull Adopted Elephant Herding Optimization (SAEHO) algorithm to improve convergence and detection performance [1], [8].

After hyperparameter tuning using the optimization strategy, the proposed model was compared with conventional machine learning approaches such as Support Vector Machine (SVM), Decision Tree, and Random Forest, as well as other optimization-based methods. The comparison was conducted to evaluate improvements in convergence speed, detection accuracy, and classification error reduction. Similar machine learning–based intrusion detection approaches have been explored in IoT cybersecurity research to detect malicious network behavior and improve system reliability [10], [14].

The performance of the proposed system was measured using several evaluation metrics, including Accuracy, Precision, Recall, F1-score, False Positive Rate (FPR), False Negative Rate (FNR), and Matthews Correlation Coefficient (MCC). These metrics provide a comprehensive evaluation of classification performance, especially when dealing with imbalanced IoT security datasets [3], [9].

Experimental results indicate that the proposed CNN-DBN hybrid model with SAEHO optimization achieves higher detection accuracy and lower false positive rates compared with conventional machine learning models. The integration of the SAEHO optimization algorithm improves the convergence speed of the learning process and enhances classification stability. These findings demonstrate that combining deep learning with an efficient hybrid optimization strategy significantly improves intrusion detection performance in IoT-enabled cyber-physical systems [2], [4], [13].

Overall, the results confirm that the proposed framework provides improved detection accuracy, reduced classification error, and enhanced robustness compared with existing intrusion detection approaches.

Accuracy Comparison of Intrusion Detection Models

The proposed model was compared with traditional machine learning classifiers including SVM, Decision Tree, and Random Forest. Performance was evaluated using accuracy, precision, recall, and F1-score.

Performance Comparison Table

Model	Accuracy	Precision	Recall	F1-Score
SVM	0.90	0.89	0.88	0.88
Decision Tree	0.92	0.91	0.90	0.90
Random Forest	0.94	0.93	0.92	0.92
CNN + DBN + SAEHO (Proposed)	0.97	0.96	0.96	0.96

The results show that the proposed hybrid model achieves the highest accuracy, demonstrating the effectiveness of combining deep learning with optimization techniques for intrusion detection [1], [7].

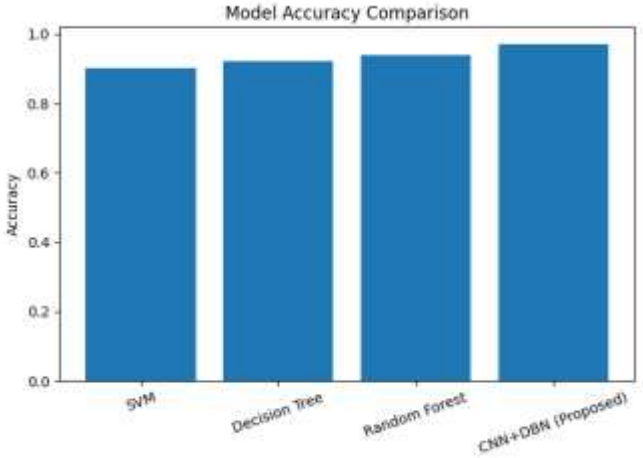

Fig. 2. Model Accuracy Comparison Bar Chart

ROC Curve Analysis

The ROC curve evaluates the relationship between True Positive Rate (TPR) and False Positive Rate (FPR). The proposed model achieved a ROC–AUC score of 0.98, indicating excellent classification capability.

The ROC curve approaching the top-left corner shows that the model effectively distinguishes between normal and malicious traffic with a low false-positive rate. ROC analysis is commonly used to assess the reliability of intrusion detection systems [6], [13].

Overall, the results demonstrate that the CNN–DBN model optimized using SAEHO improves detection accuracy and classification stability compared with traditional machine learning approaches [1], [2], [14].

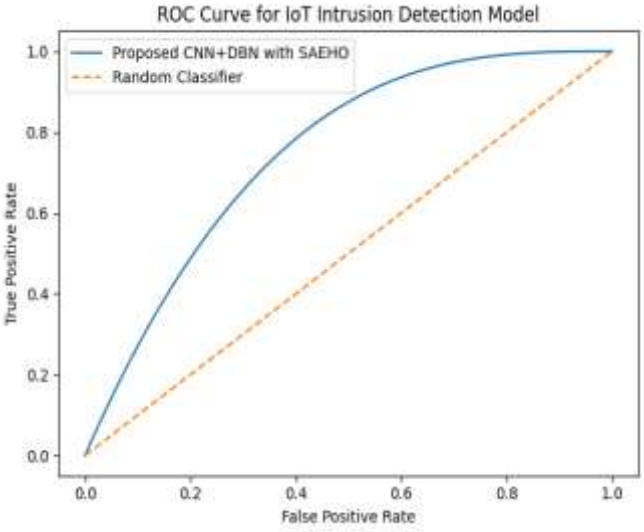

Fig. 3. ROC Curve Graph

VII.CONCLUSION AND FUTURE WORK

This project presents a hybrid deep learning-based intrusion detection framework for securing IoT-enabled cyber-physical systems. The proposed model combines Convolutional Neural Network (CNN) and Deep Belief Network (DBN) to improve feature extraction and classification performance. Hybrid deep learning approaches have been widely explored for cyber-attack detection in IoT and cyber-physical environments due to their capability to capture complex patterns in network traffic data and improve detection performance [1], [3], [10], [14]. To further enhance accuracy and convergence speed, the Seagull Adopted Elephant Herding Optimization (SAEHO) algorithm is used for parameter tuning. Optimization-based learning strategies have been shown to improve the effectiveness of deep learning-based intrusion detection systems by refining model parameters and improving classification performance [8], [9].

The experimental results obtained from standard IoT intrusion detection datasets confirm that the proposed approach performs better than traditional machine learning and existing optimization-based methods. Machine learning-based security frameworks have demonstrated strong performance in identifying cyber-attacks and mitigating security risks in IoT-enabled cyber-physical systems [3], [13]. The system achieves improved detection accuracy while reducing false positive and false negative rates, which are important factors in reliable intrusion detection systems [6], [7]. These improvements make the proposed framework suitable for real-world IoT security applications.

In future work, the system can be extended to support real-time deployment in large-scale IoT environments. Additional improvements may include integration with edge computing for faster processing and the implementation of federated learning to enhance data privacy and enable distributed collaborative learning across IoT devices [2], [4]. Furthermore, incorporating advanced deep learning architectures could further improve detection performance and system scalability in complex IoT networks [11], [12], [15]. Continuous updating of the model to adapt to emerging cyber-attack patterns can also strengthen the overall security framework.

REFERENCES

1. R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, “Hybrid DeepGCL model for cyber-attacks detection on cyber-physical systems,” Neural Computing and Applications, vol. 33, no. 16, pp. 10211–10226, Aug. 2021, doi: 10.1007/s00521-021-05785-2.
2. B. Tahir, A. Jolfaei, and M. Tariq, “Experience-driven attack design and federated-learning-based intrusion

detection in Industry 4.0," IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6398–6405, Sep. 2022, doi: 10.1109/TII.2021.3133384.

3. M. S. Abdalzaher, M. M. Fouda, H. A. Elsayed, and M. M. Salim, "Toward secured IoT-based smart systems using machine learning," IEEE Access, vol. 11, pp. 20827–20841, 2023, doi: 10.1109/ACCESS.2023.3250235.
4. P. Ruzafa-Alcázar et al., "Intrusion detection based on privacy-preserving federated learning for the industrial IoT," IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1145–1154, Feb. 2023, doi: 10.1109/TII.2021.3126728.
5. O. M. Gul, M. Kulhandjian, B. Kantarci, A. Touazi, C. Ellement, and C. D'Amours, "Secure industrial IoT systems via RF fingerprinting under impaired channels with interference and noise," IEEE Access, vol. 11, pp. 26289–26307, 2023, doi: 10.1109/ACCESS.2023.3257266.
6. F. Skopik, M. Wurzenberger, G. Höld, M. Landauer, and W. Kuhn, "Behavior-based anomaly detection in log data of physical access control systems," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 4, pp. 3158–3175, Jul. 2023, doi: 10.1109/TDSC.2022.3197265.
7. N. Cassavia, L. Caviglione, M. Guarascio, A. Liguori, and M. Zuppelli, "Learning autoencoder ensembles for detecting malware hidden communications in IoT ecosystems," Journal of Intelligent Information Systems, pp. 1–25, 2023.
8. "A hybrid deep learning model with self-improved optimization algorithm for detection of security attacks in IoT environment," Future Internet, vol. 14, no. 10, p. 301, 2022. [Online]. Available: https: //www.mdpi.com/1999-5903/14/10/301
9. F. Alrowais, H. G. Mohamed, F. N. Al-Wesabi, M. Al Duhayyim, A. M. Hilal, and A. Motwakel, "Cyber attack detection in healthcare data using cyber-physical system with optimized algorithm," Computers & Electrical Engineering, vol. 108, May 2023, Art. no. 108636, doi: 10.1016/j.compeleceng.2023.108636.
10. Q. Gulzar and K. Mustafa, "Hybrid cyber-attack detection model on cyber-physical systems using machine learning techniques," in Proceedings of Data Analytics and Management, A. Swaroop, Z. Polkowski, S. D. Correia, and B. Virdee, Eds., Singapore: Springer, 2024, pp. 197–214, doi: 10.1007/978-981-99-6547-2_16.
11. "Near real-time security system applied to SDN environments in IoT networks using convolutional neural network," Computer Networks, 2020. [Online].Available: https:/www.sciencedirect.com/science/article/abs/pii/S0045790620305930
12. [12] "Fusion-on-field security and privacy preservation for IoT edge devices: Concurrent defense against multiple types of hardware trojan attacks," IEEE Xplore, 2020. [Online]. Available:https:/ieeexplore.ieee.org/document/9003413
13. A. Raghuvanshi et al., "Intrusion detection using machine learning for risk mitigation in IoT-enabled smart irrigation in smart farming," Journal of Food Quality, vol. 2022, Feb. 2022, Art. no. e3955514, doi: 10.1155/2022/3955514.
14. P. Kumar, G. P. Gupta, and R. Tripathi, "Toward design of an intelligent cyber-attack detection system using hybrid feature reduced approach for IoT networks," Arabian Journal for Science and Engineering, vol. 46, no. 4, pp. 3749–3778, Apr. 2021, doi: 10.1007/s13369-020-05181-3.
15. "P2IDF: A privacy-preserving based intrusion detection framework for software defined Internet of Things-Fog (SDIoT-Fog)," in Adjunct Proceedings of the 2021 International Conference on Distributed Computing and Networking, 2021. [Online]. Available: https:/ /dl.acm.org/doi/abs/10.1145/3427477.3429989