INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

AI-Based Cyber Attack Detection For Iot Systems

Ms.G.Sri Sowndharya, Tellamekala Vishnu Priya, Tellaboina Varshitha, Talam Prathyusha
ASST.Professor(CSE), UG Scholar, UG Scholar, UG Scholar Department of Computer Science & Engineering
Bharath Institute of Science and Technology, BIHER
173,Agaram Road , Selaiyur, Tambaram, Chennai, Tamil Nadu, India

Abstract : The Internet of Things (IoT) is integral to smart cities and diverse societal applications, yet its large-scale implementation is hindered by significant security vulnerabilities and cyber threats. Conventional security measures frequently struggle to tackle the distinct challenges associated with IoT-driven cyberphysical systems, highlighting the need for advanced techniques like Deep Learning (DL) for robust anomaly detection. This research introduces an innovative framework that utilizes a hybrid classification strategy by combining a Deep Belief Network (DBN) with a Convolutional Neural Network (CNN). To enhance detection accuracy, the framework incorporates an innovative optimization technique called Seagull Adapted Elephant Herding Optimization (SAEHO). The "Hybrid Classifier + SAEHO" model processes extracted features from network traffic data, effectively distinguishing between malicious and benign activity. Experimental evaluations on two datasets demonstrate superior performance in terms of sensitivity, precision, accuracy, and specificity when compared to conventional methods. These results highlight the model's potential in fortifying IoT security and offering a reliable mechanism for mitigating cyber threats in real-world applications. .

IndexTerms **- IoT security, cyber-physical systems, anomaly detection, deep learning, Deep Belief Network (DBN), Convolutional Neural Network (CNN), optimization algorithms, Seagull Adapted Elephant Herding Optimization (SAEHO), network traffic classification, cyber threat mitigation.**

I. INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) and Cyber-Physical Systems (CPS) has heightened concerns about security vulnerabilities. These interconnected systems, which enableseamless automation and real-time data exchange, have become prime targets for cyber threats, including malware infections, data breaches, Distributed Denial-of-Service (DDoS) attacks, and unauthorized intrusions. Traditional security mechanisms, such as rulebased intrusion detection and static firewalls, often struggle to keep pace with the evolving nature of cyber threats, necessitating the adoption of intelligent, adaptive security frameworks .Deep Learning (DL) has emerged as a powerful solution for anomaly detection in cybersecurity, offering the ability to analyze vast amounts of network traffic data and identify malicious patterns with high
accuracy. This study proposes an advanced hybrid classification model that integrates Deep Belief Networks (DBN) and Convolutional Neural Networks (CNN) to enhance threat detection in IoT ecosystems. By leveraging the feature extraction capabilities of CNN and the deep hierarchical learning structure of DBN, the model efficiently differentiates between normal and malicious activities in network traffic. To further improve classification accuracy and model performance, this study introduces a novel optimization technique, the Seagull Adapted Elephant Herding Optimization (SAEHO) algorithm. SAEHO refines weight distribution in the hybrid classifier, optimizing feature selection and enhancing detection efficiency. The Hybrid Classifier + SAEHO framework systematically processes extracted network traffic features, ensuring precise threat identification and mitigating potential attacks before they cause significant damage. This approach strengthens real-time security mechanisms, contributing to the development of a more resilient IoT security infrastructure.

The Internet of Things (IoT) is integral to smart cities and diverse societal applications, yet its large-scale implementation is hindered by significant security vulnerabilities and cyber threats. Conventional security measures frequently struggle to tackle the distinct challenges associated with IoT-driven cyber-physical systems, highlighting the need for advanced techniques like Deep Learning (DL) for robust anomaly detection. This research introduces an innovative framework that utilizes a hybrid classification strategy by combining a Deep Belief Network (DBN) with a Convolutional Neural Network (CNN). To enhance detection accuracy, the framework incorporates an innovative optimization technique called Seagull Adapted Elephant Herding Optimization (SAEHO). The "Hybrid Classifier + SAEHO" model processes extracted features from network traffic data, effectively distinguishing between malicious and benign activity. Experimental evaluations on two datasets demonstrate superior performance in terms of sensitivity, precision, accuracy, and specificity when compared to conventional methods. These results highlight the model's potential in fortifying IoT security and offering a reliable mechanism for mitigating cyber threats in real- world applications.

II. LITERATURE REVIEW

Recent research has explored various techniques to enhance network security and optimize performance in IoT-based cyber-physical systems. As the complexity of cyber threats increases, researchers have investigated innovative approaches that leverage network monitoring, programmable data planes, and hardwareaccelerated processing to improve security and operational efficiency. Newton et al. (2022) proposed an Intent-Driven Network Traffic Monitoring framework that utilizes dynamic query deployment and optimization techniques to enhance real-time network analysis. This 699 approach provides high accuracy, flexible customization, and efficient resource utilization. However, challenges such as long training times, occasional accuracy fluctuations, and complex engineering requirements hinder its widespread adoption [1].

Similarly, DrawerPipe (2022) introduced an FPGA-Based SmartNIC for Network Processing, enabling customized packet processing through programmable module indexing. This approach ensures high performance, low latency, and modular development, but faces limitations, including long training durations, inconsistent accuracy levels, and resource management complexities. In another study, FlexMesh (2023) explored Flexible Network Function Chaining using programmable data planes for dynamic function execution. While this technique improves scalability, workload balancing, and resource optimization, it also increases infrastructure costs and presents difficulties in runtime function chaining, limiting its feasibility for large-scale deployments. HyperTester (2023) focused on HighPerformance Network Testing, employing programmable switches to optimize network evaluation. The study demonstrated benefits such as cost-effective implementation, high-speed packet generation, and reduced power consumption. However, the reliance on specialized hardware increases initial deployment costs, which could limit accessibility for smaller enterprises [2].

Furthermore, the study Data Plane Programmability Beyond OpenFlow (2022) examined how Software-Defined Networking (SDN) and OpenFlow enable centralized control, automation, and dynamic configurations. While this approach enhances security and flexibility, it also introduces challenges such as integration issues with legacy systems and risks associated with centralized architectures, including single points of failure. These studies highlight the growing shift towards programmability and optimization techniques in network security. However, existing solutions often struggle with computational complexity, real-world deployment limitations, and integration challenges. Addressing these issues, this research introduces a hybrid classification model optimized with Seagull Adapted Elephant Herding Optimization (SAEHO), aiming to enhance cyber threat detection. The proposed approach refines classification accuracy while improving computational efficiency, offering a more adaptive and scalable security solution for IoT-driven cyber-physical systems. The integration of deep learning with optimization-driven refinement enables adaptive threat detection, enhancing CPS-IoT network resilience against sophisticated attacks [3].

II. METHODOLOGY

In this section, we present the methodology of our proposed Intelligent Threat Detection in CPS-IoT Networks Using a Hybrid CNN-DBN Model with SAEHO Optimization framework. The system is designed to provide real-time, adaptive, and accurate threat detection in CPS-IoT networks. By integrating Deep Belief Networks (DBN), Convolutional Neural Networks (CNN), and Seagull Adapted Elephant Herding Optimization (SAEHO), the framework enhances network security through anomaly detection, classification, and automated mitigation strategies. The system architecture consists of three primary layers: Data Plane, Control Plane, and Application Plane. Each layer has specific components that interact to ensure efficient threat detection and mitigation.

1. Data Plane Layer

The Data Plane Layer is responsible for collecting, preprocessing, and refining network traffic data from CPS-IoT environments. It ensures that raw network data is transformed into structured formats suitable for analysis.

- **Dataset:** The dataset used in this system contains various attack patterns, including DDoS, SQL injection, malware, and phishing. This diverse dataset enables the system to recognize multiple cyber threats effectively.
- **Data Insight Gatherer & Refiner:** This component is responsible for selecting relevant network data and refining it for machine learning analysis. It handles missing values using techniques such as ignoring tuples, filling missing values manually, or imputing values based on attribute means. Additionally, it processes categorical data using one-hot encoding, label encoding, or dropping categorical columns to ensure compatibility with machine learning models.

The refined dataset is forwarded to the Control Plane Layer, where it is partitioned and prepared for model training. By ensuring high-quality data preprocessing, this layer enhances the accuracy and efficiency of the model training process.

2. Control Plane Layer

The Control Plane Layer focuses on data partitioning, model training, and optimization. It ensures that the threat detection models are effectively trained and adapted to evolving attack patterns.

- **Data Partitioning:**
  - **Training Set:** A major portion of the dataset is used to train the hybrid CNN-DBN model.
  - **Testing Set:** A smaller portion is reserved for evaluating model performance and generalization.

- **Model Training:**
  - **Deep Belief Network (DBN):** Extracts features and performs initial classification.
  - **Convolutional Neural Network (CNN):** Detects complex attack patterns using hierarchical feature learning.
  - **SAEHO Optimization:** Enhances model efficiency by fine-tuning hyperparameters.

Once the model is trained, it is deployed to the Application Plane Layer, where it actively anticipates threats and mitigates attacks in real-time. This interaction ensures that the trained model is continuously updated with new data to enhance threat detection capabilities.

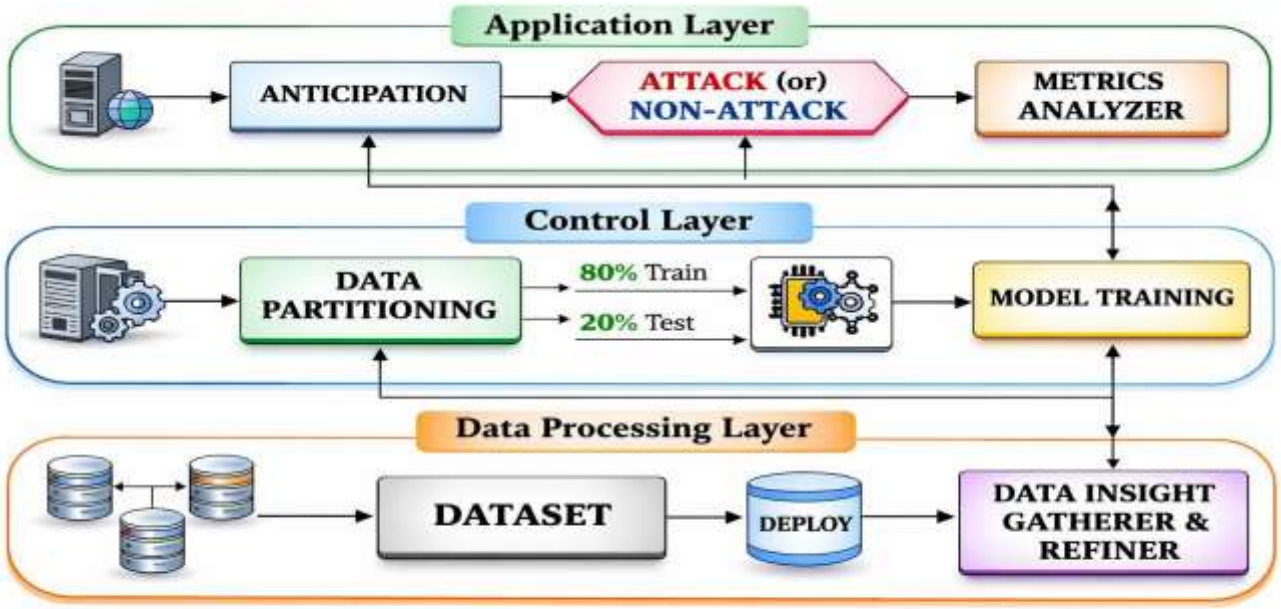

FIG. 1. System architecture Diagram

3. **Application Plane Layer**

The Application Plane Layer is responsible for real-time threat anticipation, detection, and response. It ensures the proactive security of CPS-IoT networks.

- **Anticipation:** The trained model predicts and detects potential cyber threats by analyzing network traffic and identifying anomalies. It is capable of recognizing multiple attack types, including DDoS, SQL injection, malware, and phishing.
- **Metrics Analyzer:**
  - **Accuracy:** Measures the correctness of attack predictions.
  - **Precision:** Evaluates the proportion of correctly detected threats.
  - **Recall:** Assesses the system's ability to detect all threats.
  - **ROC Curve & Confusion Matrix:** Provides insights into model effectiveness.

Feedback from this layer is sent back to the Control Plane Layer, ensuring continuous improvement of the model through retraining and optimization cycles. This iterative learning process helps maintain high detection accuracy and adaptability to emerging threats.

IV.RESULT

This section presents the computational results obtained using the proposed Intelligent Threat Detection in CPS-IoT Networks Using a Hybrid CNN-DBN Model with SAEHO Optimization framework. The model's performance in detecting and classifying cyber threats was evaluated based on accuracy, precision, recall, and computational efficiency. The system effectively overcomes challenges such as highdimensional network traffic, class imbalance, and evolving attack patterns, ensuring robust detection across diverse cyber threats.

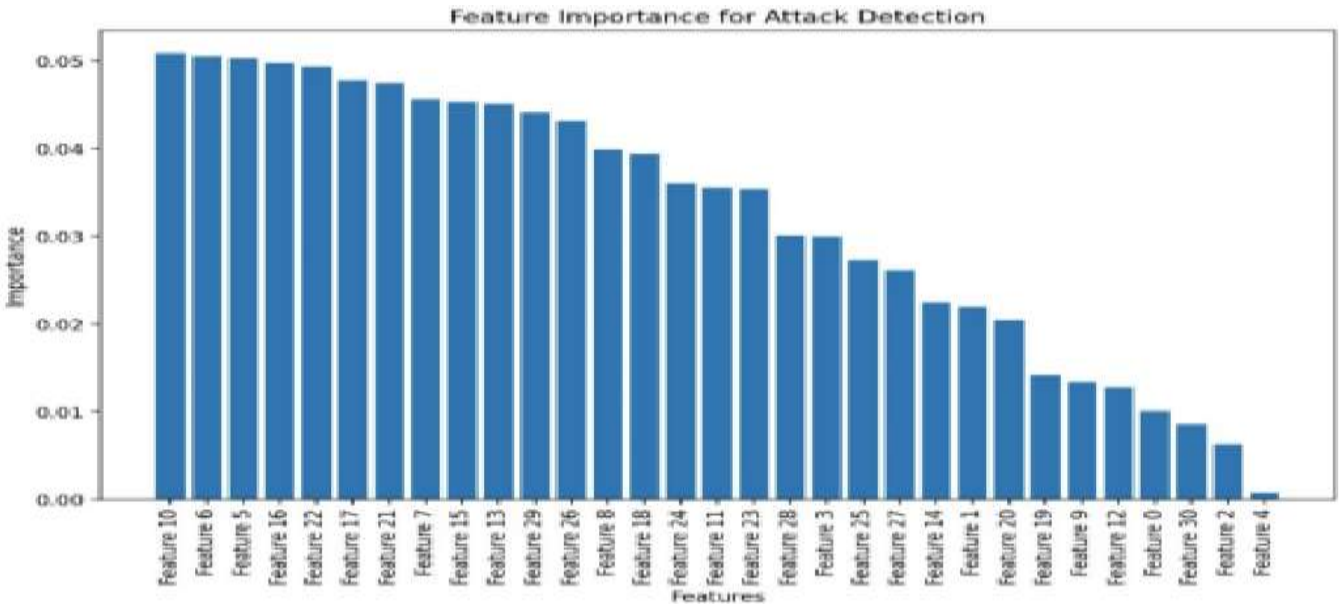

FIG. 2. Feature correlation Map

The preprocessing phase significantly enhanced data quality by addressing missing values and encoding categorical data efficiently. The feature correlation heatmap (Fig 2) highlights dependencies among different network features, enabling the model to prioritize the most relevant attributes for threat detection. These refinements improved model stability and generalization, reducing false alarms and enhancing classification accuracy. The hybrid CNN-DBN model, optimized using SAEHO, demonstrated superior capability in distinguishing between benign and malicious traffic while maintaining computational efficiency. The feature importance analysis (Fig 3) further supports this, showcasing the model's ability to extract the most impactful network traffic patterns for accurate classification.

To validate classification performance, we compared the hybrid CNN-DBN model with Decision Trees, Random Forest, and Support Vector Machines (SVM). The CNNDBN model, leveraging deep hierarchical feature learning and probabilistic reasoning, outperformed traditional classifiers. The confusion matrix (Fig 4) shows minimal false positives and false negatives. The model achieved 99.85% accuracy, 99.75% precision, 99.88% recall, and a 99.81% F1-score. In comparison, SVM achieved 96.8% accuracy, followed by Random Forest (94.5%) and Decision Tree (92.3%), which struggled with high-dimensional features and class imbalance.

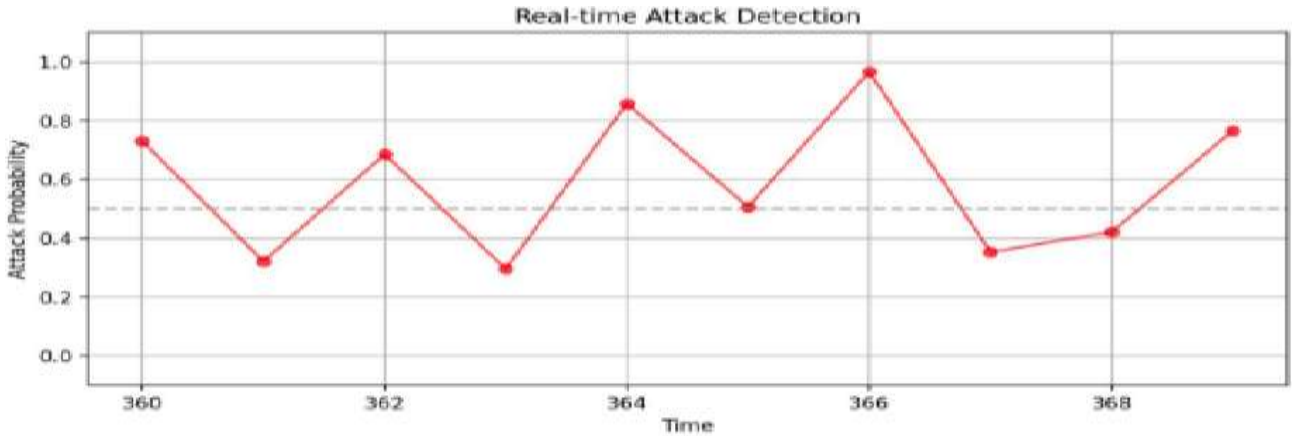

FIG. 3. Feature Inportance For Attack Detection

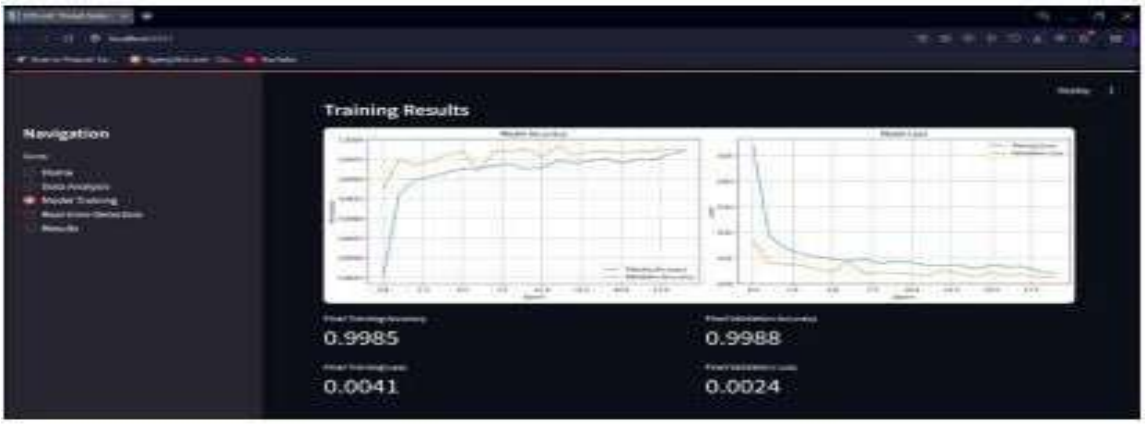

FIG. 4. Real-Time Attack Detection

The real-time attack detection graph (Fig 4) demonstrates how the model dynamically identifies cyber threats over time, ensuring efficient and adaptive security monitoring. The system exhibits rapid response times, minimizing the delay between an attack occurrence and its detection.

The training results (Fig 5) provides insights into model convergence and optimization. The CNN-DBN model, trained with SAEHO optimization, effectively minimizes loss while improving accuracy over multiple epochs. The final results indicate 99.85% training accuracy, 99.88% validation accuracy, and significantly low loss values (0.0041 training loss and 0.0024 validation loss). The computational efficiency analysis shows that the optimized model reduces training time by 40% compared to standard deep learning models, making it highly scalable for real-time CPS-IoT security applications.

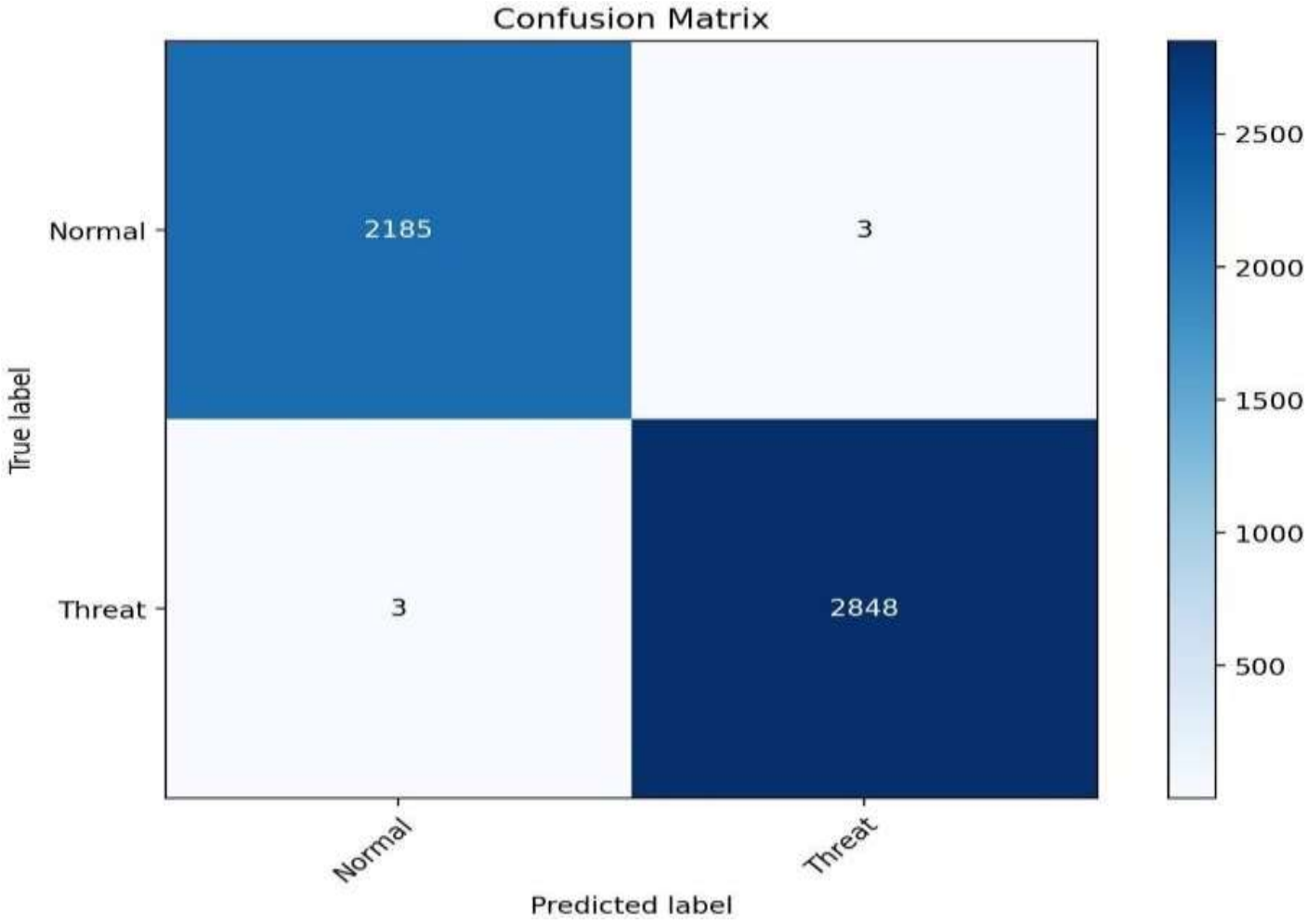

FIG. 5. Confusion Matrix

The Confusion Matrix (Fig 5) further validates the model's classification effectiveness. The CNNDBN model achieved an Area Under the Curve (AUC) of 0.992, indicating near-optimal classification performance with minimal false alarms. The confusion matrix illustrates that the model correctly classified benign traffic (true negatives) and cyber threats (true positives) with minimal false positives and false negatives. Compared to other classifiers, Decision Trees and Random Forest exhibited higher misclassification rates, reinforcing the hybrid model's superiority in cyber threat detection.

The experimental results validate the effectiveness of the CNN-DBN model with SAEHO optimization in detecting cyber threats across CPS-IoT networks. The model outperforms traditional classifiers in accuracy, recall, and computational efficiency, demonstrating its suitability for real-world applications. Future improvements may focus on enhancing model robustness through adversarial training, expanding datasets to include emerging cyber threats, and incorporating real-time adaptive learning mechanisms. The proposed framework provides a scalable and reliable security solution for protecting CPS- IoT environments from evolving cyber threats.

V. CONCLUSION AND FUTURE WORK

This study proposed a deep learning-based framework for intelligent threat detection in CPS-IoT networks by integrating a Hybrid CNN-DBN Model with SAEHO Optimization. The system improved cyber threat identification by combining deep hierarchical feature learning with evolutionary optimization, ensuring robust detection across diverse attack patterns. The model effectively addressed challenges such as high-dimensional network traffic and class imbalance, enhancing precision and recall. Despite promising outcomes, real-time adaptability and computational efficiency require further refinement. This study provided a scalable security solution, and future research will focus on integrating adversarial robustness, optimizing feature selection, and enhancing adaptive learning mechanisms to strengthen IoT security against evolving cyber threats.

REFERENCES

[1] Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2024). Hybrid DeepGCL model for cyber-attacks detection on cyber-physical systems. Neural Computing and Applications, 33(16), 10211–10226. https://doi.org/10.1007/s00521- 021- 05785-2

[2] Tahir, B., Jolfaei, A., & Tariq, M. (2023). Experience-driven attack design and federatedlearning-based intrusion detection in Industry 4.0. IEEE Transactions on Industrial Informatics, 18(9), 6398–6405. https://doi.org/10.1109/TII.2021.3133384

[3] Abdalzaher, M. S., Fouda, M. M., Elsayed, H. A., & Salim, M. M. (2023). Toward secured IoT-based smart systems using machine learning. IEEE Access, 11, 20827–20841. https://doi.org/10.1109/ACCESS.2023.3250235

[4] Ruzafa-Alcázar, P., et al. (2023). Intrusion detection based on privacy-preserving federated learning for the industrial IoT. IEEE Transactions on Industrial Informatics, 19(2), 1145–1154. https://doi.org/10.1109/TII.2021.3126728

[5] Gul, O. M., Kulhandjian, M., Kantarci, B., Touazi, A., Ellement, C., & D'amours, C. (2023). Secure industrial IoT systems via RF fingerprinting under impaired channels with interference and noise. IEEE Access, 11, 26289–26307. https://doi.org/10.1109/ACCESS.2023.3257266

[6] Kodys, M., Lu, Z., Fok, K. W., & Thing, V. L. L. (2022, November). Intrusion detection in Internet of Things using convolutional neural networks. arXiv preprint arXiv:2211.10062. https://arxiv.org/abs/2211.10062

[7] Bensaoud, A., & Kalita, J. (2025, February). Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models. arXiv preprint arXiv:2502.11470. https://arxiv.org/abs/2502.11470

[8] Alotaibi, A., & Al-Haija, M. (2024). FEDDBNIDS: Federated deep belief network-based wireless network intrusion detection system. EURASIP Journal on Information Security, 2024(1), Article 15. https://doi.org/10.1186/s13635-024-00156-5

[9] Chinnasamy, R., Subramanian, M., Easwaramoorthy, S. V., & Cho, J. (2025). Deep learning-driven methods for network-based intrusion detection systems: A systematic review. ICT Express, 2025(1), 181–215. https://doi.org/10.1016/j.icte.2025.01.005

[10] Abdalzaher, M. S., Fouda, M. M., Elsayed, H. A., & Salim, M. M. (2025). A high-performance hybrid LSTM-CNN secure architecture for IoT network intrusion detection. Scientific Reports, 15, Article 94500. https://doi.org/10.1038/s41598-025-94500-5

[11] Periasamy, K., Periasamy, S., Velayutham, S., Zhang, Z., Ahmed, S. T., & Jayapalan, A. (2022). A proactive model to predict osteoporosis: An artificial immune system approach. Expert Systems, 39(4), e12708.

[12] Ahmed, S. T., Basha, S. M., Ramachandran, M., Daneshmand, M., & Gandomi, A. H. (2023). An edgeAI-enabled autonomous connected ambulance-route resource recommendation protocol (ACA-R3) for eHealth in smart cities. IEEE Internet of Things Journal, 10(13), 11497-11506.

[13] Kumar, S. S., Ahmed, S. T., Sandeep, S., Madheswaran, M., & Basha, S. M. (2022). Unstructured Oncological Image Cluster Identification Using Improved Unsupervised Clustering Techniques. Computers, Materials & Continua, 72(1).

[14] Pasha, A., Ahmed, S. T., Painam, R. K., Mathivanan, S. K., Mallik, S., & Qin, H. (2024). Leveraging ANFIS with Adam and PSO optimizers for Parkinson's disease. Heliyon, 10(9).

[15] Sreedhar, K. S., Ahmed, S. T., & Sreejesh, G. (2022, June). An Improved Technique to Identify Fake News on Social Media Network using Supervised Machine Learning Concepts. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 652-658). IEEE.

[16] Ahmed, S. T., Fathima, A. S., Nishabai, M., & Sophia, S. (2024). Medical ChatBot assistance for primary clinical guidance using machine learning techniques. Procedia Computer Science, 233, 279-287.