JOURNAL OF SOFT COMPUTING AND DATA MINING
e-ISSN: 2716-621X

JSCDM

Vol. 6 No. 1 (2025) 333-346
https://publisher.uthm.edu.my/ojs/index.php/jscdm

An Artificial Intelligence of Things Intrusion Detection Framework for Mitigating Cyber and Ransomware Threats in IoT Networks

Shayma Wail Nourildean[1]*, Wafa Mefteh[1], Ali Mohsen Frihida[1]

[1] *National Engineering School of Tunis, University of Tunis El-Manar, TUNISIA*

*Corresponding Author: shayma.wail@enit.utm.tn

DOI: https://doi.org/10.30880/jscdm.2025.06.01.022

Article Info

Received: 2 May 2025
Accepted: 25 June 2025
Available online: 30 June 2025

Keywords

Internet of Things (IoT), Artificial Intelligence of Things (AIoT), Intrusion Detection Systems (IDS), cyberattack, deep learning

Abstract

An Artificial Intelligence of Things (AIoT) is an emerging discipline applicable across several sectors, offering a multitude of advantages. AIoT which integrates Artificial Intelligence (AI) with Internet of Things (IoT) technology to establish an intelligent network of networked devices, services, and systems. A notable challenge in AIoT security is the presence of multiple vulnerabilities. There were various methods to take advantage of vulnerabilities and conduct IoT attacks. All cyberattacks occur via network connectivity, unless one takes into account cyber-physical attacks. IDS (Intrusion Detection System) handle network traffic via devices within an IoT network. It serves as a protective barrier, capable of identifying threats and safeguarding the network against intrusions and malicious attacks. IDS serves as the essential instrument for addressing network intrusions and a range of attacks within contemporary computer network systems. This study aimed to build an efficient IDS using an ensemble model. It builds and trains an ensemble model for time-series or sequence-based classification. It uses 1D convolution layers for feature extraction, and combining predictions from different models utilizing voting rule classifiers. The model is evaluated using standard classification metrics and visualized using a confusion matrix. The testing is done with 80:20 for two data sets (IoTID20 and CIC-IoT2023 with Ransomware attacks), which include the most important types of cyberattacks. This ensemble model is examined and compared with deep learning models like (RNN, DAENN, GRU, LSTM, CNN, BiLSTM, and DNN) in terms of Precision, Recall, Accuracy, and F-Score for both binary classifications and multiple classifications of attacks. The findings show that the proposed ensemble model performed better than the other models, with accuracy and reliability reaching 94.63% and 99.99% for CIC-IoT2023 and IoTID20 datasets, respectively. Area Under the Curve (AUC) reached to 0.9459 for CIC-IoT2023 and 0.9993 for IoTID20 which indicate the better performance.

1. Introduction

An AIoT is an emerging discipline applicable across several sectors, offering a multitude of advantages. AIoT integrates AI with IoT technology to establish an intelligent network of networked devices, services, and systems. IoT is a network of interconnected sensors, software, and different technologies that provide data collection and exchange via the Internet [1]. AIoT is a relatively new phrase that combines the two prominent concepts: AI and

IoT. In an AIoT, new technologies can also be integrated to further increase their impact. Such technologies include Deep Learning (DL), blockchain, and machine Learning (ML) [2].

AIoT interlinks physical items and devices by providing them with sensory and cognitive capabilities, therefore facilitating their collaboration. They transmit information to convey their assessments. AIoT technologies facilitate the transformation of previously non-intelligent items into intelligent ones by interlinking them to the Internet through various embedded devices, Internet protocol sensor networks communication protocols and their applications [3][4].

In cybersecurity, confidentiality, availability, and integrity are widely recognized principles. Various attacks from different external or internal sources are revealed in the IoT network [5]. IoT intrusion refers to an unauthorized behavior or action that affects the IoT system. An attack that causes any sort of harm to the availability and confidentiality of information is classified as an intrusion [6]. An Intrusion Detection System (IDS) is a computer system that monitors and analyzes network data flow to detect malicious activities and report them to the network administrator.

Recently, DL technology is considered one of the hot fields within artificial intelligence. It is regarded as an AI function that mimics the human brain's data processing. Applications based on IoT are the targets of cyber-kinetic attacks. These attacks harm not only human lives but also physical well-being and the natural environment. Intrusion detection technologies are a potential way to reduce the impact of cyberattacks. In IoT-based smart environments, an efficient IDS for detecting new attacks is necessary. IDSs are designed to monitor hosts or networks for security breaches and alert administrators upon detection. An IDS is a device, physical or software-based, that detects malicious activity on a network and triggers an alert. IDSs serve as vigilant eyes to identify common types of cyberattacks, including Denial of Service attacks, phishing, malware, Man-in-the-Middle attacks, and Ransomware attacks. tack [11],[12].

This paper aims to build an efficient IDS using an ensemble model. It constructs and trains this model for time-series or sequence-based classification. It employs 1D convolutional layers for feature extraction and combines predictions from different models. The proposed ensemble merges predictions from CNN, DT, CatBoost, and KNN by summing their probabilities or predictions for each class. It then makes a final decision based on the class with the highest combined score. Additionally, it imports metrics likely used later in the code to evaluate the ensemble's performance. Testing is conducted on two datasets (IoTID20 and CIC-2023), which include the most significant types of cyberattacks. In this paper, the CIC-IoT2023 dataset is combined with a Ransomware dataset, representing a critical IoT cyberattack. The ensemble model was tested for multiple and binary classifications, showing improved system performance. These codes were written in Python, and the results were evaluated based on recall, accuracy, F-score, precision, ROC curve, and confusion matrix.

The rest of the paper is organized as follows: Section 2 presents the Related work within the IoT cyberattacks field, Section 3 presents the Research Method and includes the theoretical Concepts of the model. Section 4 presents the results, along with a discussion, and Section 5 provides the conclusion.

2. Literature Review

IoT security faces several serious challenges, one of which is the numerous vulnerabilities in the network. Vulnerabilities and attacks on Internet of Things devices can be exploited in various ways. Unless we consider cyber-physical attacks, every cyberattack occurs through the interconnectedness of our networks. IoT devices are systems with limited computing capabilities. IoT applications and Industrial Control Systems (ICS) are targets of cyber-kinetic attacks. Such attacks pose risks to human life, physical well-being, or the environment. Cyber-kinetic assaults on critical infrastructure based on the Internet of Things are often complex, involving various approaches and techniques. New cyberattacks occur daily, making it extremely difficult to prevent all of them. However, initial defense strategies are crucial for reducing the impact of both existing and potential future attacks. These strategies include intrusion detection and intrusion prevention methods, respectively. Common types of IoT cyberattacks include Botnets, Brute force, Man in the Middle, Denial of Service, Eavesdropping, Firmware and Credential attacks, Privilege escalation, and Ransomware. re.

2.1 Intrusion in IoT Network

When attacks on the IoT remain undetected for a lengthy period of time, they result in serious disruptions to service, which in turn leads to financial loss. In addition to this, it has the potential to compromise one's identity. IoTs Real-time intrusion detection is absolutely necessary to improve the dependability, safety, and profitability of IoTs enabled services [13].

Identification of harmful operations that are carried out against information systems is what is meant by the term "intrusion detection." [14].

IDS is responsible for monitoring the internet traffic that is transmitted between all of the devices that are part of an Internet of Things network. In addition to identifying potential threats and safeguarding the network from malicious assaults and unauthorized access, it serves as a line of defense. IDS are the key instrument that are utilized in modern computer network systems to combat network intrusion and other threats. IDS are responsible for monitoring the Internet of Things network, identifying any illegal incursions that may occur inside it. When it finds both internal and external assaults, intrusion detection systems (IDS) will either produce an alert or create attack flags [15]. IDS for IoT could be classified as host based IDS, network based IDS, anomaly based IDS, and distributed IDS as shown in Fig. 1 [5].

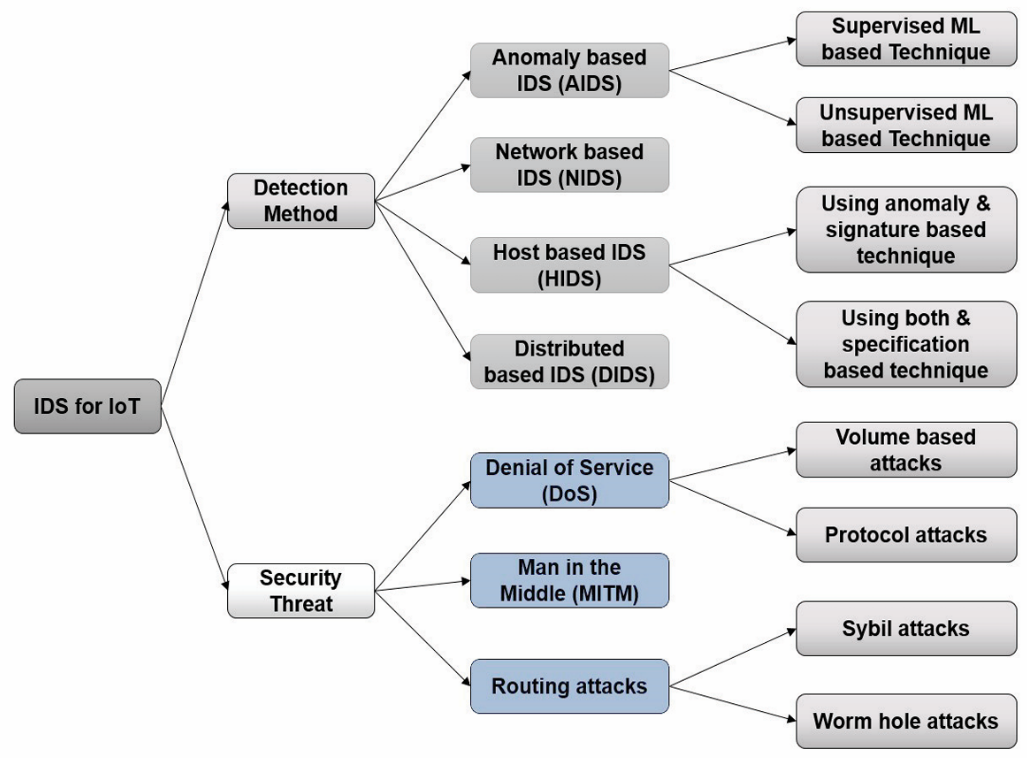


Fig. 1 *IoT based IDS [5]*

Different machine learning (ML) and deep learning (DL) algorithms have been utilized to build IDS to detect malicious activities in IoT networks.

2.2 Related Work

IDSs are crucial in the process of detecting attacks. Upon the discovery of such conduct, the administrator may additionally get alerts. Diverse deep learning and machine learning methodologies were examined to efficiently manage and classify intrusions [1]. Deep learning (DL) is presently regarded as Gold Standard which has progressively emerged as the predominant computational methodology in the domain of machine learning. A key advantage of deep learning is its capacity to process extensive datasets [16]. Furthermore, DL models surpass traditional ML methods in performance and accuracy due to its capability to autonomously extract features from extensive datasets [1]. AI generally integrates human behavior and intelligence into machines or systems. Consequently, deep learning may be regarded as a fundamental technique of artificial intelligence, serving as an edge for the development of intelligent systems and automation [7].

In the IoT context, the implementation of IDS cannot adequately address specific security concerns. The IDS aims to monitor the network activities indicative of possibly harmful network assaults. The majority of intrusion prevention and detection systems research has concentrated on cloud computing. The goal of IDS is to identify illegal access by intruders [5].

In [17]A classification model based on Deep Neural Networks (DNN) had been implemented against some machine learning models for two separate datasets. The outcomes indicate that the precision of deep learning models outperforms regression-based algorithms.

In [1], an automated IDS for IoT networks utilizing deep learning methods had been presented. This model comprises a Recurrent Neural Network with Gated Recurrent Units (RNN-GRU), which is trained and evaluated using the ToN dataset for many metrics like precision, F-score, recall, and accuracy against many sophisticated deep and conventional machine learning methodologies. The outcomes of the study indicated that the suggested system attains 98% accuracy for application layer datasets and 99% accuracy for network flow datasets.

In [13]An IDS-based innovative Deep Learning utilizing a four-layer fully connected network has been introduced. It identified different types of attacks and achieved 93.5% accuracy.

In [18], a hybrid metaheuristic-deep learning methodology had been examined to improve intrusion detection in IoT systems, utilizing an ensemble of recurrent neural networks (RNNs). Various kinds of attacks in IoT systems are discerned by the use of GRU and LSTM models using three publicly accessible datasets: IoT-23, CICIDS2017, and UNSW-NB15. The results of this study demonstrated that the suggested model performed better than all existing methods for accuracy and precision.

In [19], a CNN-BiLSTM model utilizing attention mechanisms is created to identify malicious request risks. The experimental findings demonstrate that the suggested model exceeds the existing solution regarding model robustness. The suggested platform identified various attacks and investigated the accuracy of detection of 90.01%.

This study creates an ensemble model that combines predictions from deep and machine learning models. This ensemble model has been examined on datasets combined with ransomware attacks, which are among the most significant cyber IoT attacks. These ransomware attacks aren't studied for different machines and deep learning models. Previous studies didn't examine the IoT2023 dataset, which includes various types of cyberattacks.

The challenges and gaps in previous studies on ML-based IDS using the IoTID20 dataset include:

- Limited focus on specific attack types: Some studies focus on specific attack types, such as DoS, MITM, and scanning attacks, while neglecting other types of attacks that can occur in IoT environments, like Ransomware attacks, which are among the most significant cyber IoT threats.
- Lack of comparison with traditional methods: Some studies do not compare their ML and DL-based IDS models with traditional intrusion detection methods, making it difficult to assess the true effectiveness of the proposed approaches.
- Limited Exploration of Ensemble Techniques: While some studies utilized ensemble techniques, there is a lack of comprehensive exploration and comparison of different ensemble methods for IoT intrusion detection.
- Limited Diversity of Datasets: While some studies utilized the IoTID20 dataset for evaluation, there is a lack of diversity in the datasets used for testing ML-based IDS, such as the IoT2023 dataset and the Ransomware attacks dataset. This may limit the generalizability of the proposed models to real-world IoT environments.

3. Research Methods

In IoT-based smart environments, an efficient IDS to detect new attacks is necessary. The paper aims to build an ensemble model of deep learning models in order to improve the IDS accuracy, resulting in improved reliability of the system.

The proposed ensemble model combines predictions from CNN, DT, Catboost, and KNN models by summing their probabilities or predictions for each class. It then makes a final prediction based on the class with the highest combined score. Finally, it imports metrics that are likely used in later parts of the code to evaluate the ensemble's performance. This improvement had been examined for two datasets (IoTID23 combined with Ransomware dataset and IoTID20 dataset) with traditional deep learning models (DNN) [17], Long Short-Term Memory (LSTM) [20], (GRU) [21], Convolutional Neural Networks (CNN) [22], Deep Auto Encoder NN (DAENN) [23], KNN [24]). This model had been tested for multiple and binary classifications.

The choice of dataset plays a pivotal role in both IDS types, with signature-based IDSs using offline datasets and anomaly-based IDSs relying on real-time online datasets [25]. To encourage the development of security analytics tools for use in actual Internet of Things operations, CIC-IoT2023 and IoTID20 presented an innovative and comprehensive Internet of Things attack dataset. In an Internet of Things topology comprising 10^5 devices, 33 attacks are carried out to achieve this goal. DDoS assaults, DoS attacks, Recon attacks, Web-based attacks, Brute Force attacks, Spoofing attacks, and Mirai attacks are the seven categories that these attacks fall under. Lastly, every assault is carried out by malicious Internet of Things devices.

In this paper, the CIC-IoT2023 dataset was combined with the Ransomware dataset, which represented one of the important IoT cyberattacks. Ransomware is a significant threat to IoT security because it encrypts and prevents access to crucial files [14]. The proposed IDS processing steps are presented as follows and shown in Fig. 2.

1. Preprocessing pipeline and Feature selection to check the structure and completeness of the data.
2. The dataset is divided into training and testing subsets with a data allocation of 80:20, resulting in 20% of the data in the test set, leaving 80% for training.
3. Reshapes the data for compatibility with the CNN model.
4. Building the ensemble model (CNN, DT, Catboost, KNN) as follows:
   a. Each model gives probability estimates for each class.
   b. These are stored as arrays with shape [samples x classes].
   c. Sums the probability scores from all four models for each class.

   d. Then, it selects the highest combined score class as the predicted label for that sample.
   e. res_data holds all predicted class indices.
5. Compiling the Model.
6. Loads the best saved model for evaluation.
7. Predicts the class probabilities for the test set.
8. Computes metrics to evaluate the model (Precision, F1-score, Accuracy, Recall) on the test set.
9. builds and trains an ensemble model for time-series or sequence-based classification. It uses 1D convolution layers for feature extraction. The model is evaluated using standard classification metrics and visualized using a confusion matrix.
10. This ensemble model is tested against (DNN), (LSTM), (GRU), (CNN), (DAENN), and (RNN)) for binary and multiple classifications.

As a result, this ensemble approach adds up the predicted probabilities from multiple models. The class with the highest total score wins. This is a soft voting ensemble, useful when you want to combine models with diverse strengths.

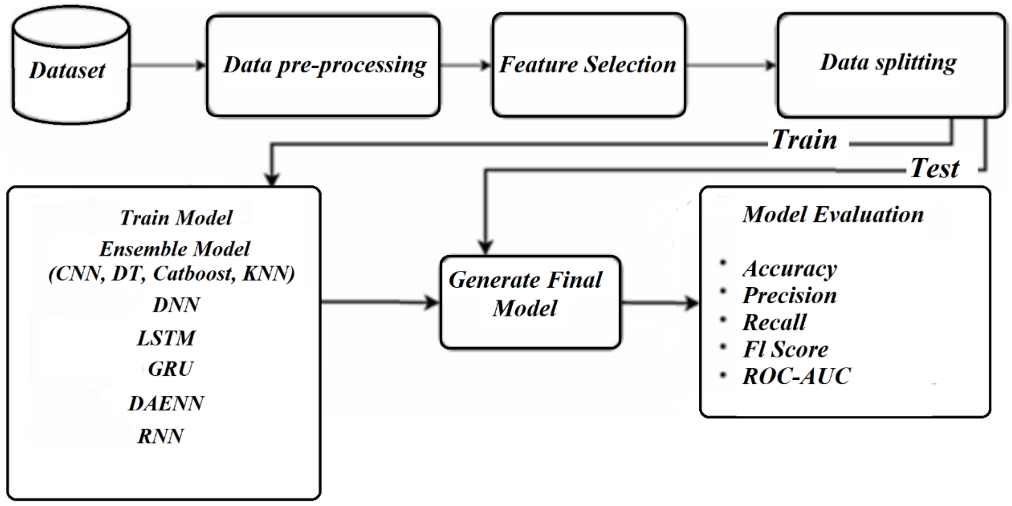


Fig. 2 *General block diagram of the proposed IDS model*

4. Results and Discussion

The Python programming language was utilized in this study for empirical experiments. The Sklearn library is employed to develop machine learning models. It is built on top of other foundational libraries such as matplotlib, SciPy, and NumPy. Scikit-learn offers a range of learning algorithms through a consistent and user-friendly API, facilitating the efficient implementation of numerous deep learning techniques, including regression, dimensionality reduction, clustering, and classification. The classifiers' quality was assessed using three IoT data sets, using 55 of the most significant factors. The outcomes are depicted as follows:

The IDS precision, F-score, recall, and accuracy were assessed employing the ensemble model on the CIC-IoT2023 dataset, as seen in Fig. 3.

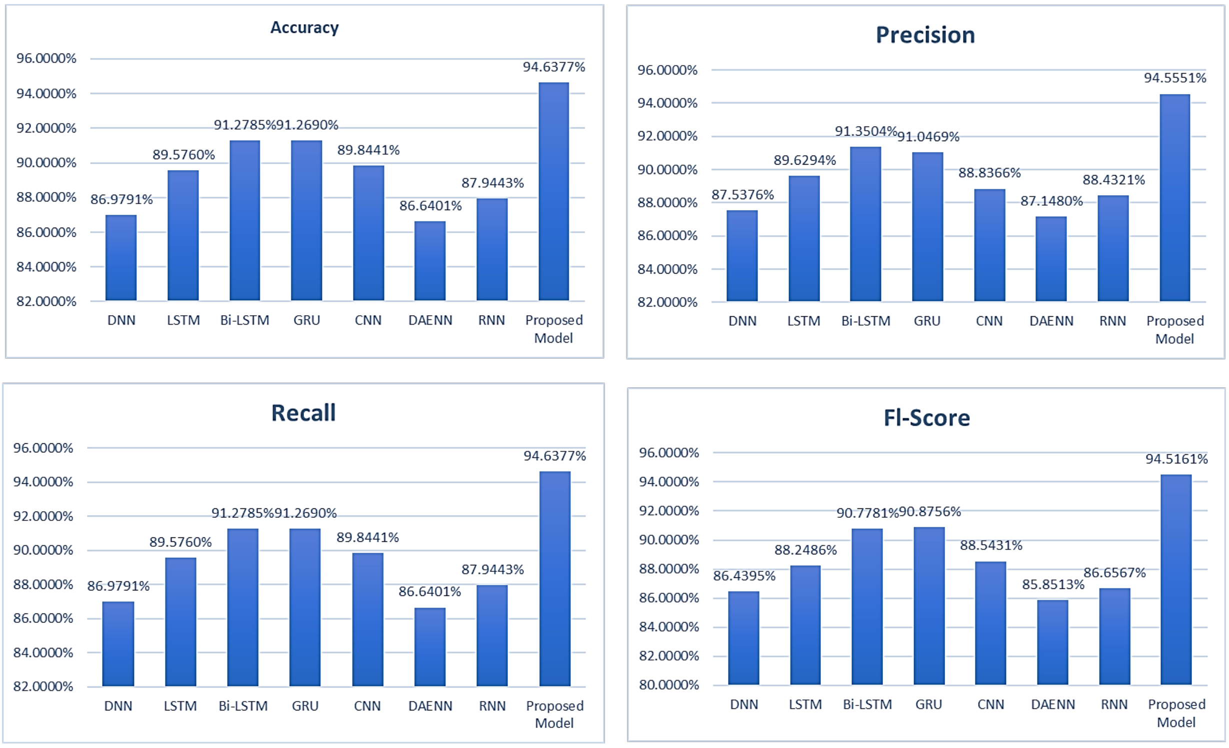


Fig. 3 *IoT2023 models performance metrics*

As shown above, the proposed ensemble model had outperformed other models to 94.6377% which indicates better learning of data patterns, possibly a hybrid or optimized architecture and Effective regularization or feature extraction strategies.

The IDS precision, Fl-score, recall and accuracy were employing the ensemble model on the IoTID20 dataset, as seen in in Fig. 4.

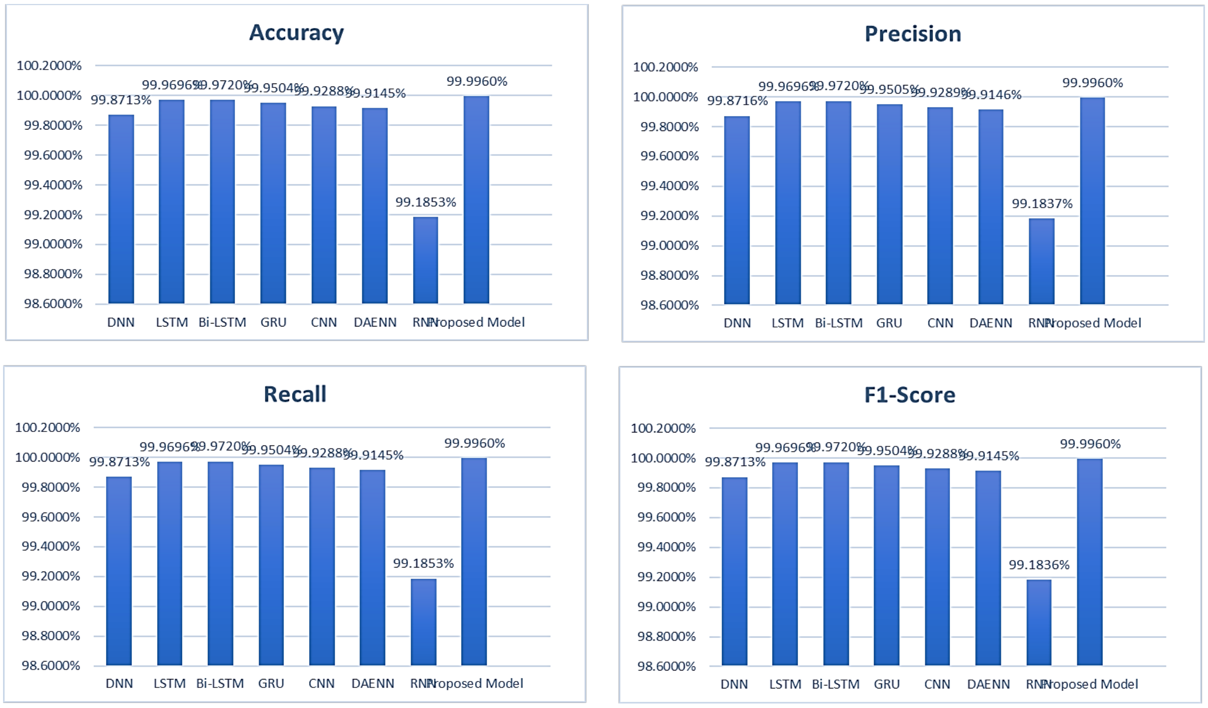
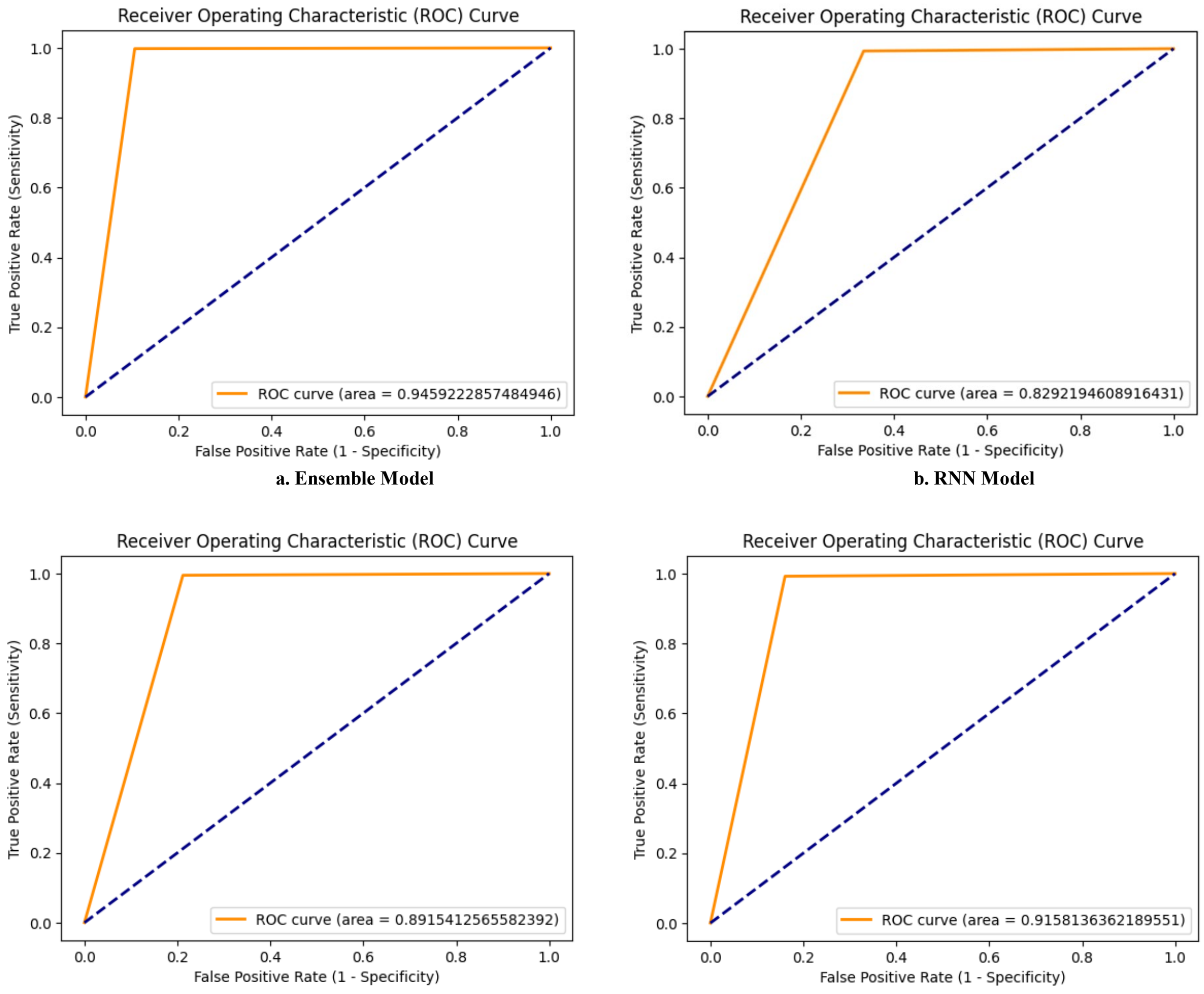


Fig. 4 *IoTID20 models performance metrics*

As shown above, the Proposed Model consistently outperforms all other models to 99.9960% across all four metrics, while DAENN performs the worst in this comparison. The other models (DNN, LSTM, Bi-LSTM, GRU, CNN, RNN) have very close results with marginal differences, indicating strong but similar performance.

The Receiver Operating Characteristic (ROC) curve is a classifier's performance graphical representation at various classification thresholds. It is commonly used to evaluate binary classifiers but can also be extended to multiclass classification. On the other hand, the Area Under the Curve (AUC) is a numerical value representing the overall performance of a binary classification model by measuring the area under the ROC curve. It is a powerful tool for model evaluation, offering a comprehensive view of a model's discriminative ability. When AUC reached to 1.0, the model represented the perfect classifier.

The ROC curves to examine the detection model performance in order to distinguish between normal behavior and intrusions (malicious activity) have been determined for this ensemble model in IoT2023 and IoTID20 datasets are shown in Fig. 5. and Fig. 6. respectively.

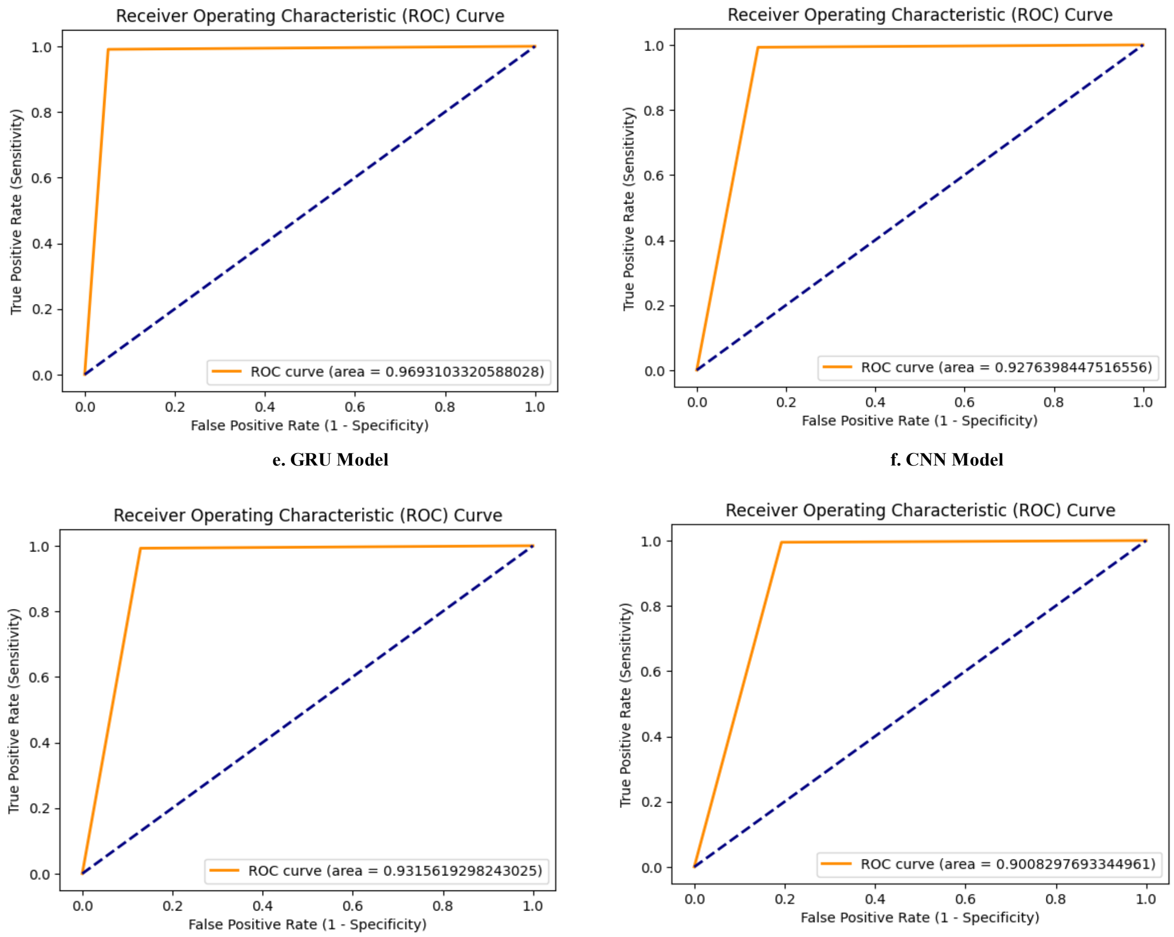


a. Ensemble Model

b. RNN Model

c. DNN Model

d. LSTM Model



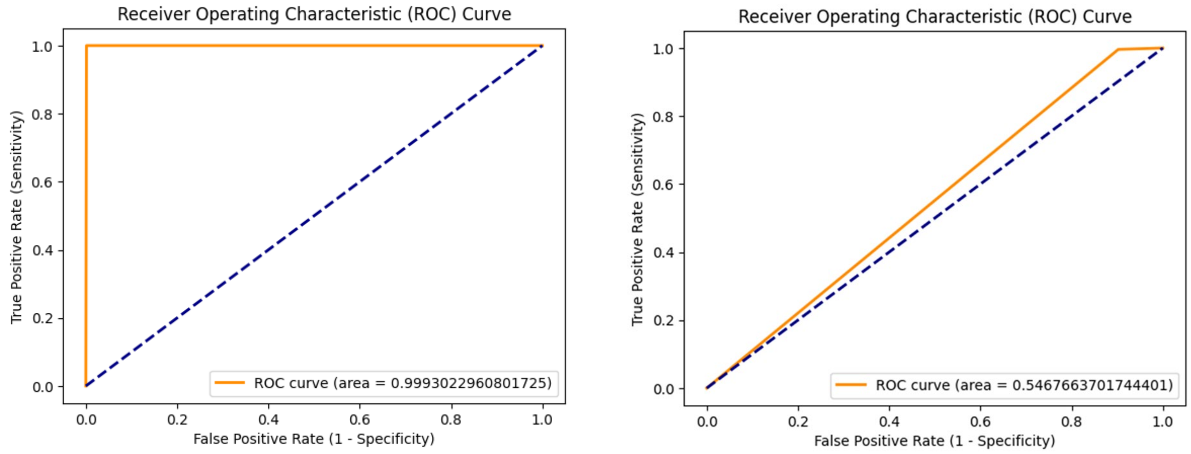
e. GRU Model

f. CNN Model

g. Bi-LSTM Model

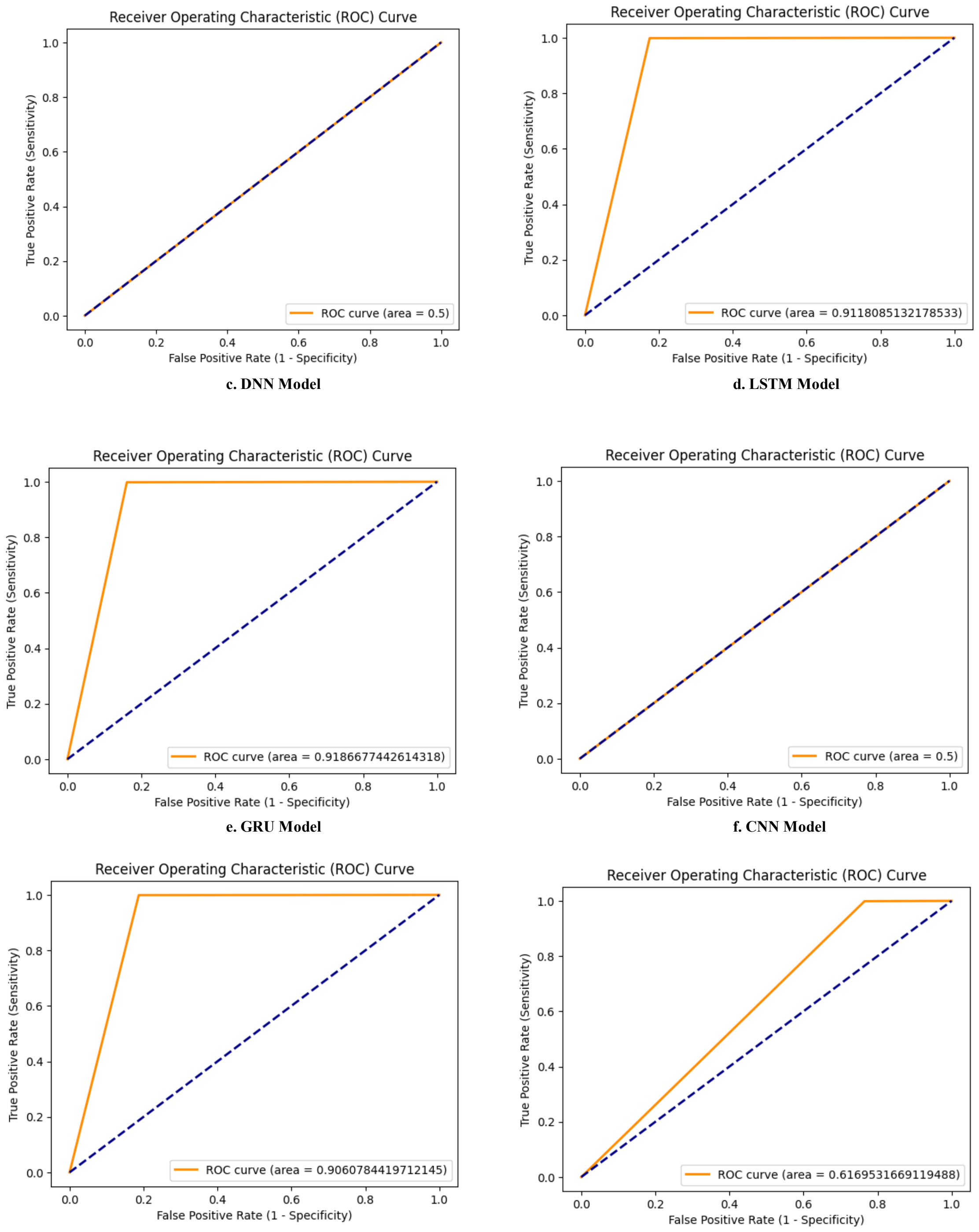
h. DAENN Model

Fig. 5. *ROC for the proposed model against traditional DL models for IoT2023*



a. Ensemble Model

b. RNN Model



c. DNN Model

d. LSTM Model

e. GRU Model

f. CNN Model

g. Bi-LSTM Model

h. DAENN Model

Fig. 6. *ROC for the proposed model against traditional DL models for IoTID20*

From Fig. 5 and Fig. 6, this ensemble model had the AUC closer to 1 which it is 0.9459 for CIC-IoT2023 and 0.9993 for IoTID20 resulting in a powerful tool for model evaluation, offering a comprehensive view of a model's discriminative ability because when AUC reached to 1.0, the model represented the perfect classifier indicating the better performance.

The proposed ensemble model and the evaluation metrics for the two datasets (CIC-IoT2023 and IoTID20) for multiple classification are shown in Table 1.

Table 1 *Evaluation metrics*

CIC-IoTID2023				
Model	Accuracy	Precision	Recall	F1-Score
DNN	86.9791%	87.5376%	86.9791%	86.4395%
LSTM	89.5760%	89.6294%	89.5760%	88.2486%
Bi-LSTM	91.2785%	91.3504%	91.2785%	90.7781%
GRU	91.2690%	91.0469%	91.2690%	90.8756%
CNN	89.8441%	88.8366%	89.8441%	88.5431%
DAENN	86.6401%	87.1480%	86.6401%	85.8513%
RNN	87.9443%	88.4321%	87.9443%	86.6567%
Proposed	94.6377%	94.5551%	94.6377%	94.5161%

IoTID20				
Model	Accuracy	Precision	Recall	F1-Score
DNN	99.8713%	99.8716%	99.8713%	99.8713%
LSTM	99.9696%	99.9696%	99.9696%	99.9696%
Bi-LSTM	99.9720%	99.9720%	99.9720%	99.9720%
GRU	99.9504%	99.9505%	99.9504%	99.9504%
CNN	99.9288%	99.9289%	99.9288%	99.9288%
DAENN	99.9145%	99.9146%	99.9145%	99.9145%
RNN	99.1853%	99.1837%	99.1853%	99.1836%
Proposed	99.9960%	99.9960%	99.9960%	99.9960%

The proposed ensemble model and evaluation metrics for existing deep learning models on two datasets (CIC-IoT2023 and IoTID20) for binary classification are presented in Table 2.

Table 2 *Evaluation metric for binary classifications*

CIC-IoTID2023				
Model	Accuracy	Precision	Recall	F1-Score
DNN	99.0520%	99.0618%	99.0520%	99.0568%
LSTM	98.9046%	99.0244%	98.9046%	98.9514%
Bi-LSTM	98.9792%	99.1122%	98.9792%	99.0286%
GRU	98.9773%	99.2251%	98.9773%	99.0560%
CNN	98.9850%	99.1046%	98.9850%	99.0302%
DAENN	99.0654%	99.0908%	99.0654%	99.0770%
RNN	98.6269%	98.6097%	98.6269%	98.6180%
Proposed	99.5557%	99.5549%	99.5557%	99.5553%

IoTID20				
Model	Accuracy	Precision	Recall	F1-Score
DNN	93.5147%	87.4500%	93.5147%	90.3807%
LSTM	98.7400%	98.7292%	98.7400%	98.6902%
Bi-LSTM	98.7320%	98.7287%	98.7320%	98.6753%
GRU	98.7784%	98.7604%	98.7784%	98.7377%
CNN	93.6978%	87.7927%	93.6978%	90.6492%
DAENN	95.0345%	94.9375%	95.0345%	93.6148%
RNN	93.7945%	92.0624%	93.7945%	91.6201%
Proposed Model	99.9912%	99.9912%	99.9912%	99.9912%

From the results of the evaluation metrics:

- The accuracy of the proposed model, which measures overall correctness and reliability, reached 94.63% and 99.99% for CIC-IoT2023 and IoTID20 datasets, respectively. The ensemble model classified 94.6% and 99.99% of the data correctly.
- This is a strong indicator that your ensemble is performing very well.
- Precision, which is the proportion of true positive detections, and Recall, which is the ability to detect all attacks, have been improved in the proposed ensemble model over the traditional deep learning models
- This ensemble model maintains a good balance between precision and recall, which is very useful in class imbalance cases.
- Making a few false positives and false negatives.
- Generalizing well to the test data.
- Consistent across different performance measures.

The study's findings demonstrated the robustness and effectiveness of the proposed ensemble model in detecting IoT attacks. It builds and trains an ensemble model for time-series or sequence-based classification. It utilizes 1D convolutional layers for feature extraction and combines predictions from multiple models.

The results of different deep learning and machine learning models for various datasets in previous studies are illustrated in Tables 3 and 4.

Table 3 *ML-Based IDS using IoTID20 dataset for binary classification*

No	Author	Classification level	Method	Best ACC
1	Alkahtani , et al, [26]	Binary	CNN LSTM CNN-LSTM	CNN-LSTM: 98.80%.
2	Yücedağ et al, [27]	Binary	PCA-MAO	99.51%
3	Albulayhi, et al, [28]	Binary	Bagging MLP J48 IBk.	Bagging: 99.81%
4	Gudla, et al, [29]	Binary	LSTMDL	Binary: 99.88%

Table 4 *ML-Based IDS using IoTID20 dataset for multivariate classification*

No	Author	Classification level	Method	Best ACC
1	Bhavsar, et al, [30]	Binary Multiple	(PCC- CNN)	Binary: 99% Multiple: 91%
2	Sarwar, et al, [31]	Binary Multiple	IDSBPSO	Binary: 99.84% Multiple: 78.46%
3	Maniriho, et al, [32]	Multiple	RF	Multiple: 99.95%
4	Dat-Thinh, et al, [33]	Binary Multiple	MidSiot	Binary: 99.99% Multiple: 99.97%
5	Alonazi, et al, [34]	Binary Multiple	LSTM ANN	LSTM Binary: 99.9% ANN Multiple: 85.7%
6	Alsulami, et al, [35]	Binary Multiple	SNN DT - BT SVM - kNN	Binary: 100% Multiple: 99.4%
7	Islam, et al, [36]	Multiple	Bi-LSTM	Multiple: 99.99%
8	Indrasiri, et al, [37]	Binary Multiple	EBF	Binary: 98.5% Multiple: 98.4%

5. Conclusion

The cyber assault targets IoT-based apps affecting human life, physical well-being, and the environment. Mitigating the impact of cyber-attacks involves intrusion detection technologies. IDS serves as the essential tool for addressing network intrusions and various cyber threats in modern computer network systems. Deep learning and machine learning technologies are prominent topics in the field of artificial intelligence. The paper aims to build an efficient IDS using an ensemble model. It constructs and trains a hybrid model for time-series or sequence-based classification. It uses 1D convolutional layers for feature extraction and combines predictions from different models using voting rule classifiers. The proposed ensemble model merges predictions from CNN, DT, Catboost, and KNN models by summing their probabilities or predictions for each class. It then makes a final prediction based on the class with the highest combined score. Finally, it imports metrics likely used in later parts of the code to evaluate the ensemble's performance. The model is evaluated using standard classification metrics and visualized with a confusion matrix. Testing is conducted with an 80:20 split for two datasets (IoTID20 and CIC-2023 with Ransomware attacks), which include the most significant types of cyberattacks. This ensemble model is examined and compared with other deep learning models (DNN, DAENN, GRU, LSTM, BiLSTM, CNN, and RNN) in terms of precision, accuracy, recall, and F1-score for both binary and multi-class attack classification. The results show that the proposed ensemble model outperformed other models, achieving reliability rates of 94.63% and 99.99% for CIC-IoT2023 and IoTID20 datasets, respectively. AUC is a powerful evaluation tool, providing a comprehensive view of a model's discriminative ability. AUC scores reached 0.9459 for CIC-IoT2023 and 0.9993 for IoTID20, indicating superior performance.

Acknowledgement

The authors would like to thank the Faculty of *National Engineering School of Tunis, University of Tunis El-Manar*, for its support.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *Shayma Wail, Ali Mohsen Frihida;* ***data collection:*** *Wafa Mefteh;* ***analysis and interpretation of results:*** *Shayma Wail, Ali Mohsen Frihida, Wafa Mefteh;* ***draft manuscript preparation:*** *Shayma Wail Nourildean. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] Khan, N. W., et al. (2023). A hybrid deep learning-based intrusion detection system for IoT networks. Mathematical Biosciences and Engineering, 20(8), 13491–13520. https://doi.org/10.3934/mbe.2023602

[2] Kataria, A., Rani, S., & Kautish, S. (2024). Artificial intelligence of things for sustainable development of smart city infrastructures (Vol. Part F3420, No. March). Springer. https://doi.org/10.1007/978-3-031-68427-2_10

[3] Resul Daş, M. Z. G. (2021). Analysis of cyber-attacks in IoT-based critical infrastructures. International Journal of Information Security Science, 8(4), 122–133.

[4] Nourildean, S. W. (2020). ZigBee-based wireless sensor network topologies using one and multiple coordinators. Periodicals of Engineering and Natural Sciences, 8(3), 1625–1640. https://doi.org/10.21533/pen.v8i3.1591.g648

[5] Sicato, J. C. S., Singh, S. K., Rathore, S., & Park, J. H. (2020). A comprehensive analysis of intrusion detection systems for IoT environment. Journal of Information Processing Systems, 16(4), 975–990. https://doi.org/10.3745/JIPS.03.0144

[6] Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets, and challenges. Cybersecurity, 4(1). https://doi.org/10.1186/s42400-021-00077-7

[7] Sarker, I. H. (2021). Deep learning: A comprehensive overview on techniques, taxonomy, applications and research directions. SN Computer Science, 2(6), 1–20. https://doi.org/10.1007/s42979-021-00815-1

[8] Elrawy, M. F., Awad, A. I., & Hamed, H. F. A. (2018). Intrusion detection systems for IoT-based smart environments: A survey. Journal of Cloud Computing, 7(1), 1–20. https://doi.org/10.1186/s13677-018-0123-6

[9] Alosaimi, S., & Almutairi, S. M. (2023). An intrusion detection system using BoT-IoT. Applied Sciences, 13(9). https://doi.org/10.3390/app13095427

[10] Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial intelligence in cybersecurity. International Journal of Engineering Research and Advanced Technology, 6(5), 1–7. https://doi.org/10.4018/978-1-6684-8098-4.ch022

[11] Vanin, P., et al. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. Applied Sciences, 12(22). https://doi.org/10.3390/app122211752

[12] Nourildean, S. W., & Mohammed, Y. A. (2023). IoT-based wireless sensor network improvement against jammers using ad-hoc routing protocols. International Journal of Interactive Mobile Technologies, 17(7), 133–147. https://doi.org/10.3991/ijim.v17i07.38587

[13] Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. Computers, 34(12), 1–17. https://doi.org/10.1016/j.iot.2024.101336

[14] Odeh, A., & Taleb, A. A. (2022). IoT security challenges and intrusion detection systems. Encyclopedia of IoT, 52541, 1–10.

[15] Eric, G., & Jurcut, A. (2022). Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets. Sensors, 22, 1–33.

[16] Alzubaidi, L., et al. (2021). Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. Springer International Publishing, 8(1). https://doi.org/10.1186/s40537-021-00444-8

[17] Bayraci, S., & Susuz, O. (2019). A deep neural network (DNN) based classification model in application to loan default prediction. Theoretical and Applied Economics, XXVI(4), 75–84.

[18] Sanju, P. (2023). Enhancing intrusion detection in IoT systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks. Journal of Engineering Research, 11(4), 356–361. https://doi.org/10.1016/j.jer.2023.100122

[19] Yang, X., Peng, G., Zhang, D., & Lv, Y. (2022). An enhanced intrusion detection system for IoT networks based on deep learning and knowledge graph. Security and Communication Networks, 2022, Article ID 4748528. https://doi.org/10.1155/2022/4748528

[20] Arifin, D. W. S., Wijaya, A. K., Nariswari, R., Yudistira, I. G. A. A., Suwarno, & Faisal. (2023). Long short-term memory (LSTM): Trends and future research potential. International Journal of Emerging Technology and Advanced Engineering, 13(5), 24–35. https://doi.org/10.46338/ijetae0523

[21] Dey, R., & Salem, F. M. (2017). Gate-variants of gated recurrent unit (GRU). Midwest Symposium on Circuits and Systems, 784, 1597–1600.

[22] Ghosh, A., Sufian, A., Sultana, F., Chakrabarti, A., & De, D. (2019). Fundamental concepts of convolutional neural network. Springer, 172. https://doi.org/10.1007/978-3-030-32644-9_36

[23] Di, J., & Wang, L. (2018). Application of improved deep auto-encoder network in rolling bearing fault diagnosis. Journal of Computer and Communications, 6(7), 41–53. https://doi.org/10.4236/jcc.2018.67005

[24] Sun, J., Du, W., & Shi, N. (2018). A survey of kNN algorithm. Information Engineering and Applied Computing, 1(1), 1–10. https://doi.org/10.18063/ieac.v1i1.770

[25] Thabit, F., Can, O., Abdaljlil, S., & Alkhzaimi, H. A. (2024). Enhanced an intrusion detection system for IoT networks through machine learning techniques: An examination utilizing the AWID dataset. Cogent Engineering, 11(1), Article ID 2378603. https://doi.org/10.1080/23311916.2024.2378603

[26] Alkahtani, H., & Aldhyani, T. H. H. (2021). Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms. Complexity, 2021, Article ID 5579851. https://doi.org/10.1155/2021/5579851

[27] Karamollaoğlu, H., Yücedağ, İ., & Doğru, İ. A. (2022). A hybrid PCA-MAO based LSTM model for intrusion detection in IoT environments. ResearchSquare. https://www.researchsquare.com/article/rs-2357212/latest.pdf

[28] Albulayhi, K., Al-Haija, Q. A., Alsuhibany, S. A., Jillepalli, A. A., Ashrafuzzaman, M., & Sheldon, F. T. (2022). IoT intrusion detection using machine learning with a novel high-performing feature selection method. Applied Sciences, 12(10). https://doi.org/10.3390/app12105015

[29] Gudla, S. P. K., Bhoi, S. K., Nayak, S. R., Singh, K. K., Verma, A., & Izonin, I. (2022). A deep intelligent attack detection framework for fog-based IoT systems. Computational Intelligence and Neuroscience, 2022, Article ID 6967938. https://doi.org/10.1155/2022/6967938

[30] Din, Z., Jambari, D. I., Yusof, M. M., & Yahaya, J. (2021). Challenges in IoT technology adoption into information system security management of smart cities: A review. Advances in Science, Technology and Engineering Systems Journal, 6(2), 99–112. https://doi.org/10.25046/aj060213

[31] Chandhar, K., Singh, D. P., Alanya-Beltran, J., Akram, S. V., Kothandaraman, D., & Tiwari, M. (2023). Enhanced anomaly detection system for IoT based on improved dynamic SBPSO. In 2023 International Conference on Artificial Intelligence and Smart Communication (AISC) (pp. 544–547). https://doi.org/10.1109/AISC56616.2023.10084980

[32] Maniriho, P., Niyigaba, E., Bizimana, Z., Twiringiyimana, V., Mahoro, L. J., & Ahmad, T. (2020). Anomaly-based intrusion detection approach for IoT networks using machine learning. In International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM).

[33] Dat-Thinh, N., Xuan-Ninh, H., & Kim-Hung, L. (2022). MidSiot: A multistage intrusion detection system for Internet of Things. Wireless Communications and Mobile Computing, 2022, Article ID 9173291. https://doi.org/10.1155/2022/9173291

[34] Alonazi, W. A., Hamdi, H., Azim, N. A., & El-Aziz, A. A. A. (2022). SDN architecture for smart homes security with machine learning and deep learning. International Journal of Advanced Computer Science and Applications, 13(10), 917–927. https://doi.org/10.14569/IJACSA.2022.01310108

[35] Alsulami, A. A., Abu Al-Haija, Q., Tayeb, A., & Alqahtani, A. (2022). An intrusion detection and classification system for IoT traffic with improved data engineering. Applied Sciences, 12(23). https://doi.org/10.3390/app122312336

[36] Islam, N., et al. (2021). Towards machine learning-based intrusion detection in IoT networks. Computer Materials & Continua, 69(2), 1801–1821. https://doi.org/10.32604/cmc.2021.018466

[37] Indrasiri, P. L., Lee, E., Rupapara, V., Rustam, F., & Ashraf, I. (2022). Malicious traffic detection in IoT and local networks using stacked ensemble classifier. Computer Materials & Continua, 71(1), 489–515. https://doi.org/10.32604/cmc.2022.019636