MJSAT

Malaysian Journal of Science and Advanced Technology

journal homepage: https://mjsat.com.my/

Enhancing IoT Security: A Deep Learning Approach with Feedforward Neural Network for Detecting Cyber Attacks in IoT

Arjun Kumar Bose Arnob[1], and Akinul Islam Jony*[1]

[1] *Department of Computer Science, American International University-Bangladesh (AIUB), Dhaka, Bangladesh.*

KEYWORDS

IoT
Cyber Security
FNN Network
CIC-IoT2023
Intrusion Detection

ARTICLE HISTORY

Received 23 March 2024
Received in revised form 2 August 2024
Accepted 13 August 2024
Available online 8 September 2024

ABSTRACT

A new era of connectedness has been ushered in by the increasing number of Internet of Things (IoT) devices, which present both enormous security issues and limitless opportunities for creativity. With the use of a deep learning-powered intrusion detection system (IDS), this research aims to improve IoT security. An extensive dataset of different cyberattack kinds was used to train and test a Feedforward Neural Network (FNN) for its ability to detect intrusions using the CIC-IoT2023 dataset. The FNN achieved excellent accuracy, an F1 score, and a precision score, which are encouraging results. This shows the system's capability to differentiate between legitimate and fraudulent network traffic and illustrates its potential value in protecting IoT ecosystems. However, there are certain restrictions, such as the necessity for continuing optimization and the representativeness of the dataset. This research provides knowledge regarding the efficiency of deep learning-based IDS, which is an essential step toward strengthening IoT security. This work lays the groundwork for continued initiatives to guarantee the reliability and safety of linked IoT devices in a constantly shifting threat environment as the IoT environment develops.

1. INTRODUCTION

The IoT has advanced significantly in recent years. It describes the real world as an extensive network of objects with a digital identity. These devices, including sensors, actuators, mobile phones, televisions, light bulbs, thermostats, medical equipment, smart watches, software, and other items, may need to be bigger and bigger. IoT is a concept that involves an exponentially expanding spectrum of physical items connected to the internet [1]. According to [2], IoT is growing quite quickly and is currently used in many different fields like education, health, and agriculture (e.g., [3]). By 2025, connected devices are predicted to increase daily to 30.9 billion. IoT network traffic has rapidly increased because of this phenomenon.

IoT devices continue to have severe risks despite their widespread use, including, for example, exposed network services, a lack of encryption or access control, and inadequate protection for sensitive data. As a result, attacks on IoT devices are increasing quickly, and technologies that can identify assaults are urgently needed to respond and implement remedies [4]. IoT refers to gadgets, buildings, and structures that use connected devices, sensors, and actuators. IoT devices find a growing number of applications as sensors and storage for data, and the Internet has become increasingly affordable, quick, and integrated. Since many diverse traffic classes and a lot of network traffic flow through IoT networks, such as those produced by industrial machinery, driverless cars, health sensors, smart homes, and other vital devices, this interaction presents significant difficulties. As a result, the needs of different IoT applications necessitate more security and protection, which requires accurate network traffic classification to detect assaults earlier and take appropriate countermeasures. Given the widespread use of IoT devices, malevolent manipulations could significantly impact the stability and security of the entire Internet [5]. The Mirai malware's strike serves as a crystal-clear illustration of the severity that results from using zombie IoT devices (bots) to launch a more significant DDoS attack and attests to the need

*Corresponding author:
E-mail address: Akinul Islam Jony < akinul@aiub.edu >.
https://doi.org/10.56532/mjsat.v4i4.299

for secure authentication mechanisms and appropriate traffic categorization algorithms [6, 7].

According to [8], IoT systems' complex and linked nature makes it more challenging to provide all-encompassing security. Additionally, there is a considerable risk due to the physical frailty of IoT devices in unmonitored situations. Intruders can take advantage of this weakness. Concerns regarding data privacy are increased by the vulnerability of the wireless networks linking IoT devices to eavesdropping and illegal access. If not adequately protected, the massive amount of data produced by IoT devices also presents privacy concerns, and combining IoT with other technologies makes it more difficult to ensure security and privacy across several systems. In addition, IoT devices' limited processing and power capabilities make it difficult to strike the right balance when installing comprehensive security measures. It is crucial to address these complex difficulties to guarantee IoT systems' safe and secure deployment across multiple areas. The IoT scenario entails the internet-based interconnection of a wide range of physical items and systems, giving them connectivity, software, and sensors to gather and exchange data [9].

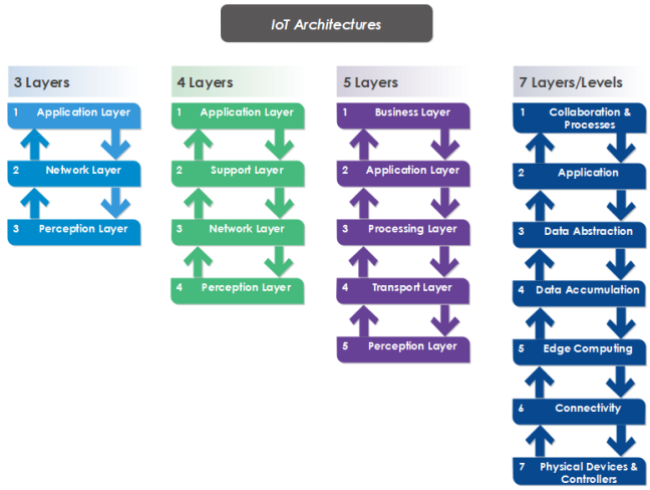

Fig. 1. IoT Layers Architecture

According to [10], Fig. 1 illustrates various IoT layer stack suggestions for the IoT architecture. Researchers have proposed different architectures with 3, 4, 5, and 7 layers (or levels).

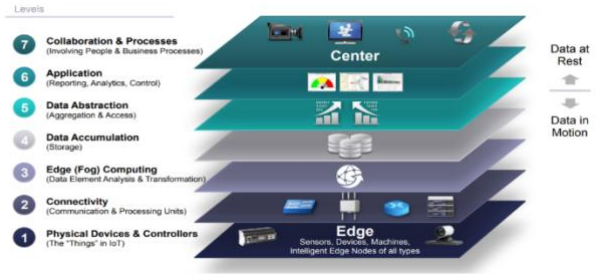

Fig. 2. CISCO's IoT Reference Model (source: [11])

Fig. 2 indicates [11] that the IoT reference model consists of seven distinct layers, each serving a particular purpose within the IoT ecosystem. At Level 1, physical devices and controllers represent tangible IoT components capable of data creation and conversion. Level 2, or the connectivity layer, uses protocols, routing, security, and analytics to guarantee dependable device-to-network communication. Edge (Fog) Computing, which does data processing close to the network edge, is introduced in Level 3. This includes data filtering, aggregation, inspection, thresholding, and event production. Data in motion is converted into data at rest at Level 4 and organized for further processing and query-based computing. Level 5, Data Abstraction, offers data virtualization and consolidation while streamlining data access by balancing diverse formats, semantics, sources, and security considerations. Level 6, the application level, analyzes data for purposes, varies between vertical markets, and provides consumers with helpful information.

Finally, Level 7, Collaboration and Processes, involves people and corporate processes and facilitates value creation through communication and collaboration. At all levels, security is prioritized, and the IoT Reference Model incorporates security features, including identity management, authentication, and encryption to provide complete security. This framework provides a formal understanding of the structure and functions of the IoT system and seeks to standardize language, ease communication, and foster collaboration within the IoT sector. This IoT reference architecture divides the IoT ecosystem into multiple tiers, each with unique functions and monitoring points, providing a solid foundation for IoT threat detection. Due to the granularity, precise and focused monitoring is possible, making identifying anomalies and potential security risks simpler. Edge (Fog) computing is also included, ensuring real-time analysis at the network edge and allowing for quick detection of questionable activity closer to its source. The model focuses on security measures at all levels, from identity management to encryption, and offers numerous layers of protection against attackers. Additionally, the approach promotes more efficient threat detection and response by unifying nomenclature and facilitating data correlation across layers. This reference model encourages a thorough strategy for IoT security and improves the ability to identify and stop IoT-related assaults quickly.

On the other hand, real-time data analysis (such as [12] and [13]) can be applied for detection purposes. Also, deep learning is a proven approach for building prediction models such as [14]. Using FNN in the context of IoT threat detection with a large dataset offers several benefits. FNNs provide a simple, practical design that can scale up to meet the requirements of an extensive dataset. In the dynamic environment of IoT security, their capacity for generalization across many attack methods is precious.

Additionally, FNNs are exceptional at automatically extracting pertinent features from complicated data, eliminating the need for time-consuming manual feature engineering. FNNs can also use parallel processing, using contemporary GPUs and distributed computing frameworks to quicken training times. The complexity of the attacks, potential data preparation needs, and the accessibility of computational resources must all be considered. FNNs are a good contender for IoT threat detection. Still, it's important to carefully compare different deep learning architectures to

determine which is best for the given dataset and security objectives.

This research ensures that the approach and findings are understood. Following the introductory overview, go to the 'Related Works' section, which includes noteworthy research and approaches used in IoT cyber-attacks. This study seeks to create an effective Intrusion Detection System (IDS) for IoT contexts using Feedforward Neural Networks (FNNs). This involves a comprehensive analysis of the CIC-IoT2023 dataset to recognize essential characteristics conducive to risk detection on IoT devices. Measurement of the given IDS effectiveness by various means is part of this research, thus guaranteeing its robustness and confidence. Applying edge computing techniques to tackle IoT problems related to safety and having complete secure controls are, among other things, taken care of in this work. The 'Methods and Materials' section follows, providing an in-depth explanation of the approach, including an overview of the dataset, how the model was used, the assessment criteria used, and the processes followed to assess the model's performance. The 'Results and Analysis' section details the findings, including model-specific evaluation metrics, learning curves, confusion matrices, ROC curves, and precision-recall curves. The 'Conclusion' section comprehensively appraises the investigation, including its implications, limitations, and recommendations for future scholarly research in this field.

2. RELATED WORKS

The authors of [15] suggest deep learning models based on convolutional neural networks (CNNs) and long short-term memory (LSTM) networks for identifying DDoS attacks in IoT networks. These models have a high accuracy of 97.16% after training on the most recent CIC-IDS2017 datasets. Deep learning models outperform conventional machine learning methods in terms of accuracy. These models can automatically learn from unstructured and diverse data, extract features, adjust to shifting network conditions, and identify novel attack types. The authors propose creating new deep-learning architectures and training techniques to address open research issues in IoT cybersecurity.

In [16], researchers used the IoT-23 dataset, which comprises network traffic information from both malware-infected Raspberry Pi devices and benign IoT devices, to undertake an experimental evaluation. To identify attacks on IoT devices, they suggested a hybrid deep learning model that focuses on dynamic analysis of attacks by running malicious binary files on devices and observing network traffic. In this novel method, op-code sequences were chosen as features for classification, and feature graphs were made to show the connections between features and samples. They used deep Eigenspace learning to decrease the dimensionality of the feature space and improve classification accuracy. An empirical analysis showed that junk code insertion assaults may be detected with 98% accuracy. The study's shortcomings, which are encouraging but call for further validation on more extensive and more diverse datasets for real-world applicability, include a tiny and self-manufactured dataset. In conclusion, the hybrid Deep Learning Model developed by the authors provides a viable way to increase IoT device security by effectively exploiting IoT-generated data.

The application of distributed deep learning techniques for IoT threat detection was applied by [17], but they need to provide the research dataset. It does, however, refer to numerous datasets that are frequently used for assessing intrusion detection systems. A CNN model achieved an accuracy of 0.9430 in an IoT micro-security add-on, and RNN-LSTM achieved mean accuracy ranging from 73.21% to 97.84% in various subsets of the Mirai and Gafgyt botnets, according to the article, which provides comprehensive accuracy data for numerous models. Data gathering from IoT devices, training deep learning models on a back-end server, and actual time implementation for attack detection are all components of the suggested method for IoT attack detection. This method uses both the processing power of IoT devices and servers. The authors claim their approach has promised to identify developing IoT assaults, especially those leveraging encrypted traffic for escape. However, potential limitations and hurdles include the requirement for strong encryption and privacy safeguards.

Authors of [18] examined the use of the Bot-IoT dataset produced at the Australian Centre for Cyber Security (ACCS) to evaluate the use of machine learning to detect cyber threats within IoT networks. This dataset, which includes valid traffic and numerous attack types like probing denial-of-service attacks and information theft, is essential for teaching machine learning algorithms to distinguish between genuine and malicious network activity. The approach used by the authors included extensive data processing steps, feature extraction using CICFlowMeter, and the application of seven different machine learning algorithms, including KNN, ID3, quadratic discriminant analysis (QDA), Random Forest, AdaBoost, multilayer perceptron (MLP), and Naive Bayes (NB). Adaboost, which achieved 100% accuracy, precision, recall, and F-measure, was the best-performing algorithm, with KNN and ID3 following behind with 99%.

In addition to providing a foundation for more sophisticated and accurate detection systems, the study emphasizes the potential of machine learning to strengthen IoT network security and the importance of diversified datasets that include both legitimate and malicious traffic for efficient algorithm training. The authors' additional contributions to the IoT security literature include improving attack detection in IoT networks, refining feature selection to increase algorithm performance, and exploring the relatively new Bot-IoT dataset. This indicates that this study offers a thorough and insightful examination of machine learning's function in identifying cyberattacks within IoT networks, highlighting the importance of different training data.

To improve the cybersecurity of computer numerical control (CNC) equipment, the article [19] presents a novel cybersecurity solution that combines deep learning algorithms with IoT devices. The authors separated the dataset into training and testing subsets by classifying a dataset of cutting signals recorded under various cutting settings into three groups. A deep neural network (DNN) model was assessed alongside conventional machine learning classifiers like KNN, artificial neural networks (ANN), and support vector machines (SVM), as well as ensemble learning techniques like random forest (RF) and eXtreme Gradient Boosting (XGBoost). The outcomes demonstrated the suggested DNN model's better performance, reaching a remarkable 99.47% classification accuracy on the test dataset. Precision and recall scores close

to one suggested reliable fake signal detection during cyberattacks. The model's superior detection abilities, particularly during attacks, were confirmed by performance evaluations using f1-scores and receiver operating characteristic (ROC) curves, with the maximum performance at 1.0.

3. METHODS AND MATERIALS

The overall methodological approach is discussed in this section, which is depicted in Fig. 3 as well.

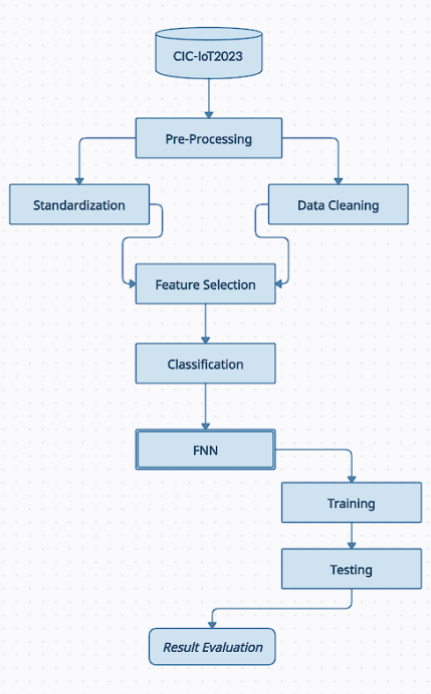

Fig. 3. Research Process

As mentioned in Fig. 3, the deep learning process on the "CIC-IoT2023" dataset encompasses multiple essential steps. The process commences with pre-processing, wherein the raw data is subjected to cleansing, normalization, and transformation to verify its appropriateness for subsequent analysis. In the standardization phase, the data is modified to have a mean of 0 and a standard deviation 1. This process ensures that feature weights are consistent and reduces the influence of certain traits. Data cleaning is the process of eliminating or rectifying errors, corruptions, copies, and incorrectly formatted data to improve the overall quality of the data. Feature selection is a process that selects the most critical variables, which helps to reduce overfitting and improve the model's accuracy. The procedure continues with classification, utilizing the chosen features in an FNN model to classify or forecast the target variable. The FNN model's performance is evaluated through the Training and Testing phases, which involve using a portion of the data for training and evaluating the model on new data. Result Evaluation assesses the model's efficacy by employing diverse metrics such as precision, recall, F1 score, and accuracy, offering valuable insights into its performance.

3.1 Dataset Overview

This paper utilizes the publicly accessible CIC-IoT2023 dataset [20], which comprises authentic network traffic from various IoT devices in typical and malicious conditions. The CIC-IoT2023 dataset was produced in collaboration between the Information Technology University of Copenhagen (ITU) and the Canadian Institute for Cybersecurity (CIC). A smart home environment comprising twenty IoT devices (cameras, thermostats, smart TVs, smart wearables, etc.) was simulated to create the dataset. Wireshark and TCPDump were utilized to capture network traffic for classification by Snort and Suricata intrusion detection systems. The dataset comprises ten days' worth of network traffic, consisting of five days of regular traffic and five days of attack traffic. The dataset consists of ten distinct varieties of DDoS attacks, namely MQTT Flood, CoAP Flood, WS-DDoS (WebSocket), Web Service Flood (SOAP), and Web Service Flood (RESTful), in addition to TCP SYN Flood, UDP Flood, HTTP Flood, HTTP Slow Post, Slowloris, MQTT Flood, CoAP Flood. The dataset comprises an estimated eighty million packets, of which sixteen million are deemed normal, and 64 million are classified as malicious. Each transmission in the dataset is accompanied by 115 characteristics, which comprise the source and destination IP addresses, protocol, payload size, and timestamp. The paper [13] executed the machine learning approach with the same dataset, where they analyzed various machine learning algorithms for the CIC-IoT2023 dataset. Besides, in [21], an LSTM-based deep learning approach is proposed based on this dataset.

Fig. 4. Dataset Overview in terms of various cyber attacks

The overall number of rows in the dataset and the corresponding attacks and their row counts are shown in Fig 4. A wide range of IoT threats thus threatens the availability and integrity of computer systems and networks in cybersecurity. Distributed Denial of Service (DDoS) attacks use several tactics, such as flooding assaults like UDP and ICMP Floods and fragmentation-based attacks. DoS attacks impair services by saturating one source with traffic. Attacks used for reconnaissance involve probing to find out about services and weaknesses. Web-based assaults target web programs with methods like SQL Injection and XSS. Brute force attacks employ a series of tests to gain unauthorized access. Spoofing refers to attacks that alter network traffic or fake entities. Finally, Mirai attacks employ tactics like GREIP Flood and UDPPlain attacks targeting IoT devices. Protecting digital assets and maintaining network stability from attacks presents unique challenges for security professionals.

Fig 5 presents a comprehensive dataset comprising 47 different features that were painstakingly gathered from network traffic data and are used as the basis for in-depth analysis and categorization. These features cover a wide range of network characteristics, from the most basic like timestamps that show when packets were captured and flow durations that show how long communication sessions lasted—to the most complex—like protocol types, packet rates, and flag information that reveal the nature and degree of network activity. Furthermore, the examination of protocols like HTTP, HTTPS, DNS, TCP, UDP, ARP, and others makes it possible to identify communication patterns and services thanks to the presence of application, transport, and link layer protocol identification. Inter-arrival times (IAT) measure the time gaps between subsequent packets, and packet length statistics, which include aggregate metrics like total sum, minimum, maximum, average, and standard deviation, provide deep insights into the distribution of packet sizes within a flow.

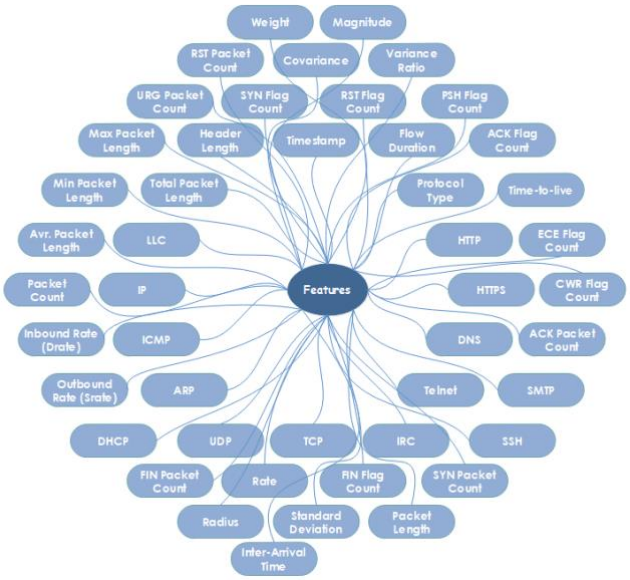

Fig. 5. Features from the network traffic

The dataset's statistical measurements, including magnitude, radius, covariance, variance, and weight, provide complex statistical viewpoints that enable a detailed analysis of packet length distributions and their interactions. The dataset's usefulness extends to network performance analysis, making it possible to evaluate network performance measures. The combined effect of these elements is significant because it gives stakeholders the ability to enhance security protocols, optimize network performance, and guarantee the dependability and effectiveness of network communications. This dataset provides a cornerstone in the toolkit needed for thorough examination and classification of networking behavior, ultimately enhancing the robustness and dependability of contemporary network infrastructures. It facilitates tasks like network monitoring, detection of breaches, and traffic engineering.

3.2 FNN

Fig 6 visually illustrates the fundamental design of an FNN. According to [22], FNNs consist of three primary layers: the input, hidden, and output layers. In an FNN, the number of layers in the input and output layers is typically the same, while the number of hidden layers and neurons within them can vary based on specific requirements. Trial and error, guided by performance considerations, is often employed to determine the optimal configuration of hidden layers and neurons. The network's architecture maps inputs, represented by offsets δ1, δ2, and δ3, to outputs in the form of hinge angles α, β, and γ, using weighted connections between artificial neurons across different layers. During training, these weights are adjusted to effectively map inputs (the offsets of block centers) to outputs (corresponding hinge angles). Each artificial neuron within the FNN is characterized by an activation function, typically nonlinear, such as the tangent sigmoid or logarithmic sigmoid, which introduces the necessary nonlinearities for complex function approximation. It is worth noting that, following the Universal Approximation Theorem, a single hidden layer FNN with a finite number of neurons can estimate continuous functions on compact subsets of $\mathbb{R}n$, where n is the number of inputs. However, determining the optimal FNN architectural configuration for a specific input-output relationship often requires a trial-and-error approach, considering factors like the number of hidden neurons and for training, utilizing the Mean Squared Error (MSE) as the performance metric and the Levenberg-Marquardt (LM) backpropagation technique due to its high efficiency and second-order convergence rate, as documented in the literature [23, 24, 25].

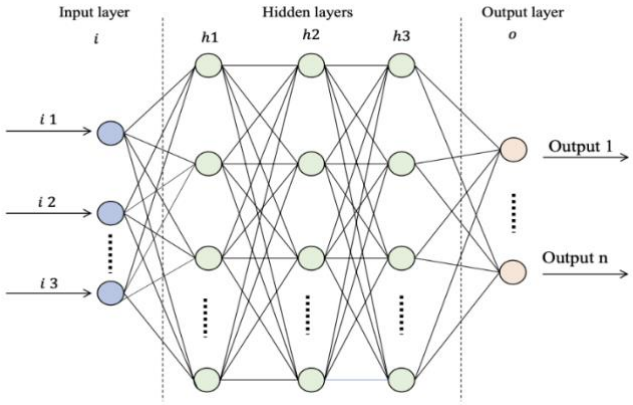

Fig. 6. Architecture Model of a Feedforward Neural Network (FNN) (source: [22])

3.3 Evaluation Metrics

The proposed model's evaluation matrices include accuracy, precision, recall, and F1-score, presented briefly below with their corresponding equations.

Accuracy: The proportion of correctly categorized packets to all packets.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (1)$$

Precision: The proportion of harmful packets accurately identified relative to all malicious packets expected.

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

Recall: The proportion of harmful packets that were accurately identified to all malicious packets.

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

F1-Score: The harmonic means of recall and precision.

$$F1 - Score = \frac{Precision + Recall}{2} \quad (4)$$

4. RESULTS AND FINDINGS

This study advances network security by demonstrating how deep learning may improve intrusion detection while also offering a thorough analysis underpinned by a strict 70-30 data split and an instructive epoch learning curve.

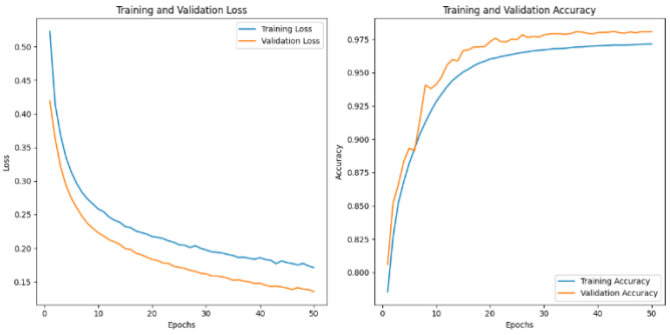

Fig. 7. Epoch curve of the proposed model

Fig 7's epoch learning curve shows FNN's training dynamics throughout 50 epochs. Notably, the curve shows quick convergence and consistent gains in validation and training accuracy, highlighting how well the model learned and generalized from the dataset. The trustworthiness of the IDS is confirmed by the near alignment of the two curves, which shows robust generalization without overfitting. Performance stabilizes after a certain point, indicating declining returns from further training.

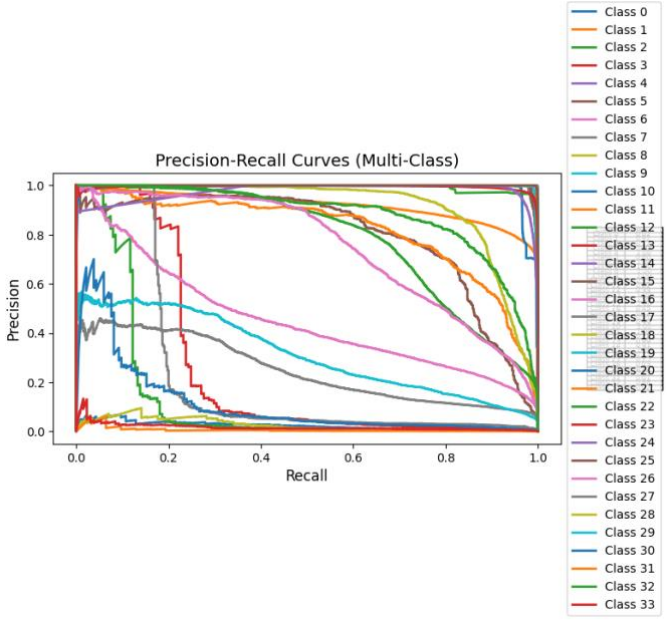

Fig. 8. Precision-Recall Curve of the proposed model

Fig 8 indicates the curve's trajectory and sheds light on how well the model can categorize various types of network traffic. This paper's proposed IDS displays outstanding precision-recall characteristics for various typical attack types, including DDoS and DoS attacks, demonstrating its powerful detection skills. It also points up opportunities for improvement, particularly in classes with lower recall and accuracy values, indicating the need for additional model improvement for those risks.

The confusion matrix shown in Fig 9, which classifies data instances into the true positive (TP), true negative (TN), false positive (FP), and false negative (FN) categories, is revealed by this matrix. These categories represent the model's capacity to accurately distinguish between positive and negative situations and its tendency for Type I (false positive) and Type II (false negative) errors. The matrix also measures performance indicators like recall, precision, and the F1-score for each class, enabling a detailed analysis of the IDS's capabilities for identifying specific threats.

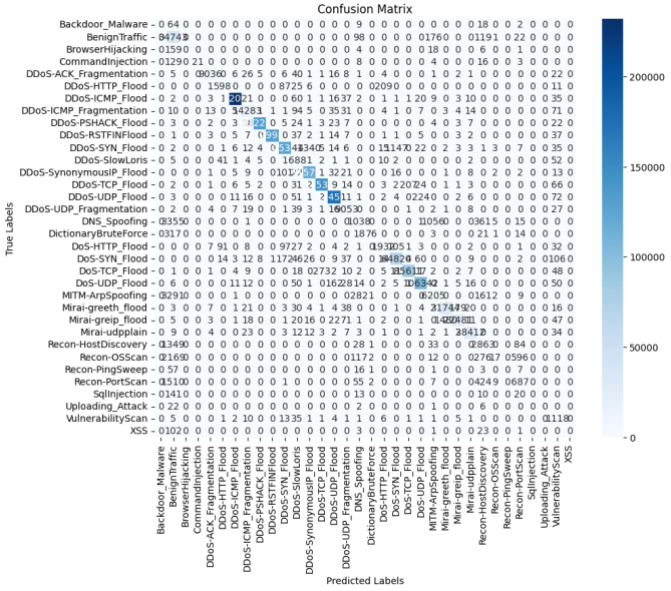

Fig. 9. Confusion Matrix

Table 1. Evaluation matrices of the proposed FNN model

Evaluation Matrices	Output (Score)
Accuracy	0.9807
F1 Score	0.9786
Recall Score	0.9807
Precision Score	0.9799

Table 1 indicates the assessment of our proposed IDS using rigorous testing and actual network traffic information. The accuracy, F1 score, recall score, and precision score of the performance metrics table highlight how well IDS can discriminate between legitimate and malicious network data. This paper's system displays its ability to achieve a harmonious balance between accurately identifying network intrusions and avoiding false positives with an exceptional accuracy of 0.9807 and an F1 score of 0.9786. Additionally, the system's recall score of 0.9807 demonstrates its dependability in identifying genuine threats, and its precision score of 0.9799 indicates its accuracy in reducing false alerts.

Table 2 presents a comparison and explains how different models for machine learning and deep learning compare in

terms of performance with our proposed Feedforward Neural Network (FNN) for IoT intrusion detection using the CIC-IoT2023 dataset.

Table 2. Comparison among various machine learning and deep learning approaches with our proposed FNN approach

Evaluation Matrices	Accuracy	F1 Score	Recall Score	Precision Score
FNN	0.9807	0.9786	0.9807	0.9799
LSTM	0.9875	0.9859	0.9875	0.9866
Random Forest	0.9916	0.9909	0.9916	0.9913
KNN	0.9380	0.9364	0.9380	0.9366
Decision Tree	0.9919	0.9920	0.9954	0.9919
Logistic Regression	0.8275	0.8034	0.8275	0.8473

The FNN showed very high levels of accuracy with a score of (0.9807). The values obtained include an F1 score of (0.9786), a recall rate of (0.9807) and a precision rating of (0.9799). These results demonstrate the FNN's ability to differentiate between legitimate and malicious network data. By comparison, the author of [13, 21] applied the Long Short-Term Memory (LSTM) approach using the same dataset and had superior accuracy (0.9875), F1 score (0.9859), recall (0.9875), and precision (0.9866).

The Decision Tree model attained an accuracy of 0.9916, an F1 score of 0.9919, a precision of 0.9883, and demonstrated exceptional recall with a score of 0.9954. The Random Forest model was very accurate and precise, with accuracy and precision equal to (0.9916). On the other hand, the performance of k-Nearest Neighbours (KNN) and Logistic Regression models was lower than that of deep learning methods. Indeed, while FNN did not beat other top-performing models in all metrics, it was more balanced by reducing false positive rates. Thus, it suits IoT security applications where simplicity, fastness, and effectiveness are key factors.

5. Conclusion and Future Work

This study explores the crucial field of intrusion detection inside the developing IoT environment. With its exponentially growing number of physically connected IoT devices, network security faces both unmatched opportunities and difficulties. By building the analysis around an extensive dataset named CIC-IoT2023, a very recent dataset of different cyberattack kinds, and by picking an FNN model for intrusion detection. Through investigation and review produced encouraging findings. With a fantastic accuracy of 0.9807 and an F1 score of 0.9786, the FNN successfully distinguished between legitimate and malicious network traffic. With a recall score of 0.9807, demonstrating its robustness in recognizing actual threats, and a precision score of 0.9799, emphasizing its precision in decreasing false positives, this emphasizes the system's ability to strike a balance among identifying network intrusions and limiting false alarms. These results demonstrate the usefulness of the IDS in protecting IoT ecosystems, with significant consequences for network security experts and researchers.

It's essential to recognize the limits of this study, though. The dataset's specific properties may impact the model's performance even though it is comprehensive and may not cover all potential IoT attack scenarios. Future studies may also improve the model's performance and investigate real-time detection capabilities. Collaboration among cybersecurity experts may enhance the sturdiness and scalability of intrusion detection systems in the constantly changing IoT environment.

Future work will be impacted by the inevitably new attack avenues that IoT technological improvements will bring forth, demanding continued research and advancement in intrusion detection systems. Additionally, using anomaly detection methods and adding more complex characteristics could improve the IDS's precision and recall even more. Additionally, to confirm the system's efficacy in real-world circumstances, real-world implementation and testing in various IoT environments are essential. This study is a significant step toward strengthening IoT security through efficient intrusion detection. Creating dependable and flexible security solutions is crucial as the IoT expands quickly. This study contributes to this ongoing effort by providing a solid framework for the defense of IoT ecosystems against various cyber threats.

Dataset Availability Statement

The dataset used in this study can be found at https://www.unb.ca/cic/datasets/iotdataset-2023.html [accessed on 12 November 2023].

References

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376.

[2] Nascita, A., Cerasuolo, F., Di Monda, D., Garcia, J. T. A., Montieri, A., & Pescapè, A. (2022, May). Machine and deep learning approaches for IoT attack classification. In IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.

[3] Alam, M. M., & Jony, A. I., (2023). Supply Chain Management Techniques Using Big Data for Agro-Based Food Products in Bangladesh. International Journal of Data Science and Big Data Analytics. 3(2), 19-34.

[4] Luong, N. C., Hoang, D. T., Wang, P., Niyato, D., Kim, D. I., & Han, Z. (2016). Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey. IEEE Communications Surveys & Tutorials, 18(4), 2546-2590.

[5] Jony, A. I., & Hamim, S. A. (2023). Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age. Journal of Information Technology and Cyber Security. 1(2), 53-67.

[6] Calabretta, M., Pecori, R., & Veltri, L. (2018, September). A token-based protocol for securing MQTT communications. In 2018 26th International Conference on Software, telecommunications, and computer networks (SoftCOM) (pp. 1-6). IEEE.

[7] Perrone, G., Vecchio, M., Pecori, R., & Giaffreda, R. (2017, April). The Day After Mirai: A Survey on MQTT Security Solutions After the Largest Cyber-attack Carried Out through an Army of IoT Devices. In IoTBDS (pp. 246-253).

[8] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685.

[9] Ibitoye, O., Shafiq, O., & Matrawy, A. (2019, December). Analyzing adversarial attacks against deep learning for intrusion detection in IoT

networks. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[10] Idrissi, I., Azizi, M., & Moussaoui, O. (2020, October). IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review. In 2020 Fourth International Conference on Intelligent Computing in Data Sciences (ICDS) (pp. 1-10). IEEE.

[11] CISCO (2014). IoT Reference Model. Accessed on September 12, 2023, from:https://dl.icdst.org/pdfs/files4/0f1d1327c5195d1922175dd77878b9fb.pdf

[12] Jony, A. I. (2016). Applications of real-time big data analytics. International Journal of Computer Applications, 144(5), 1-5.

[13] Jony, A. I., & Arnob, A. K. B. (2024). Securing the Internet of Things: Evaluating Machine Learning Algorithms for Detecting IoT Cyberattacks Using CIC-IoT2023 Dataset. International Journal of Information Technology and Computer Science (IJITCS), 16(4), 56-65.

[14] Jony, A. I., & Arnob, A. K. B. (2024). Deep Learning Paradigms for Breast Cancer Diagnosis: A Comparative Study on Wisconsin Diagnostic Dataset. Malaysian Journal of Science and Advanced Technology, 4 (2), 109-117.

[15] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., & Zhao, S. (2021). Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 14(1–2), 1-210.

[16] Sahu, A. K., Sharma, S., Tanveer, M., & Raja, R. (2021). Internet of Things attack detection using hybrid Deep Learning Model. Computer Communications, 176, 146-154.

[17] Parra, G. D. L. T., Rad, P., Choo, K. K. R., & Beebe, N. (2020). Detecting Internet of Things attacks using distributed deep learning. Journal of Network and Computer Applications, 163, 102662.

[18] Alsamiri, J., & Alsubhi, K. (2019). Internet of Things cyber attack detection using machine learning. International Journal of Advanced Computer Science and Applications, 10(12).

[19] Tran, M. Q., Elsisi, M., Liu, M. K., Vu, V. Q., Mahmoud, K., Darwish, M. M., ... & Lehtonen, M. (2022). Reliable deep learning and IoT-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification. IEEE Access, 10, 23186-23197.

[20] Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment.

[21] Jony, A. I., & Arnob, A. K. B. (2024). A long short-term memory-based approach for detecting cyber attacks in IoT using the CIC-IoT2023 dataset. Journal of Edge Computing, 3(1), 28-42.

[22] Samarakoon, S. B. P., Muthugala, M. V. J., Le, A. V., & Elara, M. R. (2020). HTetro-infi: A reconfigurable floor-cleaning robot with infinite morphologies. IEEE Access, 8, 69816-69828.

[23] Haykin, S. (2009). Neural networks and learning machines, 3/E. Pearson Education India.

[24] Hagan, M. T., & Menhaj, M. B. (1994). Training feedforward networks with the Marquardt algorithm. IEEE Transactions on Neural Networks, 5(6), 989-993.

[25] Marquardt, D. W. (1963). An algorithm for least-squares estimation of nonlinear parameters. Journal of the Society for Industrial and Applied Mathematics, 11(2), 431-441.