LNN Algorithm for IOT Intrusion Detection

GIRISH REDDY S [1], Prof. A G VISHVANATH [2]

[1] Student, Department of MCA, Bangalore Institute of Technology, Karnataka, India

[2] Professor, Department of MCA, Bangalore Institute of Technology, Karnataka, India

ABSTRACT

The growing use of Internet of Things (IoT) devices has expanded the cyber-attack surface, creating new challenges for intrusion detection. Traditional signature-based systems often fail against zero-day attacks and evolving threats. This project proposes a proactive cybersecurity model integrating Logical Neural Networks (LNN) with advanced preprocessing and real-time monitoring. By combining white box testing, enhanced threat hunting, and robust incident response, the system strengthens detection accuracy and resilience. The prototype framework captures network traffic, extracts critical features, and applies intelligent anomaly detection, achieving high precision with reduced false positives. Results demonstrate improved adaptability, scalability, and effectiveness for modern IoT environments.

1. INTRODUCTION

In today's digital ecosystem, the rapid growth of the Internet of Things (IoT) has transformed industries and daily life by interconnecting billions of devices. These devices generate immense volumes of data and enable advanced automation, decision-making, and real-time monitoring across domains such as healthcare, manufacturing, transportation, and smart homes. While this interconnectivity has created unparalleled opportunities for efficiency and innovation, it has also introduced new cybersecurity risks. Each connected device represents a potential entry point for cybercriminals, making IoT networks increasingly vulnerable to exploitation.

Traditional cybersecurity defenses, such as firewalls, antivirus software, and signature-based Intrusion Detection Systems (IDS), continue to serve as the first line of protection. However, their reliance on predefined rules and known threat signatures makes them inadequate in handling zero-day exploits, advanced persistent threats (APTs), and evolving malware. These systems often generate excessive false positives, overwhelming security analysts and slowing down response time. Moreover, IoT devices typically operate with limited computational power and memory, which restricts the use of resource-intensive security solutions. This combination of limitations underscores the urgent need for intelligent, adaptive, and proactive approaches to securing IoT networks.

One promising direction is the integration of machine learning and advanced analytical techniques into intrusion detection frameworks. Unlike traditional static defenses, machine learning-based systems can learn from patterns of network traffic and adapt to previously unseen attack vectors. Within this paradigm, the Logical Neural Network (LNN) emerges as a powerful solution. LNN combines the learning capabilities of neural networks with logical reasoning, providing not only high detection accuracy but also explainable outcomes. This balance of intelligence and interpretability enhances trust in automated security decisions and helps organizations better understand the nature of detected threats.

The proposed project builds on this concept by designing an LNN-based Intrusion Detection System specifically tailored for IoT environments. The system captures network traffic, preprocesses it to extract meaningful features, and applies the LNN model to classify activities as normal or malicious. By implementing advanced feature selection and normalization methods, the system improves detection efficiency and reduces the likelihood of false alarms. Additionally, the modular design ensures scalability, enabling seamless deployment across diverse IoT settings, from small-scale smart devices to large industrial networks.

Beyond detection, the project emphasizes a comprehensive security approach by integrating whitebox testing, proactive threat hunting, and structured incident response mechanisms.

Whitebox testing allows for in-depth examination of system logic and configurations, uncovering vulnerabilities that blackbox testing might overlook. Proactive threat hunting leverages analytics and threat intelligence to search for hidden anomalies before they escalate into full-scale attacks. Finally, a robust incident response framework ensures that, when attacks do occur, they can be contained, eradicated, and recovered from with minimal disruption.In summary, this project addresses critical challenges in IoT cybersecurity by combining advanced neural network techniques with structured defensive strategies. By focusing on accuracy, adaptability, and proactive monitoring, the system provides organizations with a resilient solution to counteract evolving cyber threats. The outcome not only contributes to academic research but also delivers practical value to industries seeking reliable and scalable security mechanisms for safeguarding IoT ecosystems.

2. RELATED WORK

The rapid evolution of cyber threats has motivated extensive research into intrusion detection, threat hunting, and incident response. Conventional methods, such as perimeter defense and signature-based detection, remain relevant but are increasingly inadequate against zero-day exploits, advanced persistent threats (APTs), and adaptive attack strategies. Researchers have therefore explored advanced techniques that combine software testing principles, data-driven models, and intelligent automation to build more resilient security systems.

Whitebox testing, traditionally used in software engineering for code verification and debugging, has emerged as a promising approach in cybersecurity. Studies highlight that whitebox testing can uncover vulnerabilities at the source code, data flow, and system architecture levels, providing visibility that blackbox testing often lacks. John Do's comprehensive review of whitebox testing techniques discussed static and dynamic analysis, symbolic execution, and concolic testing, noting their potential in strengthening system defenses by identifying flaws before exploitation. Emily Brown further expanded on this concept, emphasizing the integration of whitebox testing with threat hunting to proactively detect hidden attack vectors within networks and applications.

Threat hunting has also seen significant advancements as organizations move away from reactive defense models. Jane Smith's work on enhanced threat hunting underscored the importance of analytics, machine learning, and automation in proactively identifying anomalies. Her study demonstrated how integrating threat intelligence sources with hunting practices enables early recognition of compromise indicators. Similarly, David Lee evaluated the effectiveness of whitebox-enhanced threat hunting and incident response strategies through real-world simulations. His findings indicated improved detection accuracy and faster containment of attacks when these methods were combined, though challenges such as scalability and analyst expertise remained.

Incident response frameworks have also been a focus of prior research. Michael Johnson proposed a structured methodology covering containment, eradication, recovery, and post-incident analysis. His work highlighted the importance of predefined procedures, compliance with regulatory standards, and continuous improvement based on lessons learned. This complements proactive detection methods by ensuring organizations can not only identify threats but also recover quickly and minimize business disruption.

Parallel to these approaches, machine learning and deep learning have been widely applied to network intrusion detection, especially in the IoT domain. Ziadoon K. Maseer and colleagues introduced a hybrid deep learning model, DeepIoT.IDS, that integrated Restricted Boltzmann Machines with deep neural networks, achieving exceptional detection accuracy on complex datasets like CICIDS2017. Similarly, Bambang Susilo and Riri Fitri Sari demonstrated how deep learning algorithms significantly improve detection of denial-of-service (DoS) attacks in IoT networks, showcasing the adaptability of neural models to evolving threats. Other researchers, such as Sarah Alkadi and team, investigated preprocessing and optimization techniques, proving that data quality and model tuning are critical for effective intrusion detection.

Recent studies have also proposed lightweight and explainable detection models to address IoT constraints. Hasan et al. explored autoencoder-based feature learning for industrial IoT, improving classification accuracy on imbalanced datasets. Abdel-Basset et al. introduced Deep-IFS, which applied recurrent and attention-based mechanisms to capture long-range dependencies in IIoT traffic. While these models improved accuracy, interpretability and resource efficiency remain open challenges.

Collectively, prior research highlights the limitations of traditional defenses and the promise of integrating whitebox testing, machine learning, and structured response systems. However, most existing works focus on either detection accuracy or incident handling in isolation. Few have proposed a holistic model that unifies proactive vulnerability assessment, real-time anomaly detection, and coordinated response strategies. This project addresses that gap by combining Logical Neural Networks (LNN) with whitebox-enhanced threat hunting and robust incident response, offering a scalable, explainable, and proactive framework for IoT security.

3.PROBLEM STATEMENT

The rapid proliferation of Internet of Things (IoT) devices has revolutionized industries and daily life by enabling real-time connectivity and automation. However, this growing interconnectivity has also significantly expanded the cyber-attack surface, making IoT networks highly vulnerable to sophisticated threats such as Distributed Denial-of-Service (DDoS), botnet intrusions, and zero-day exploits. Traditional Intrusion Detection Systems (IDS), which primarily rely on signature-based or rule-driven approaches, struggle to identify novel attack patterns and often produce a high volume of false positives. Additionally, the limited computational resources of IoT devices restrict the deployment of complex security solutions, leaving networks exposed.

4.PROPOSED SYSTEM

The proposed system introduces a proactive cybersecurity framework that integrates **Logical Neural Networks (LNN)** with **whitebox testing**, **enhanced threat hunting**, and **robust incident response** to address the limitations of traditional intrusion detection methods in IoT environments. Unlike conventional systems that rely mainly on signatures or external behavior, this model combines intelligent learning with internal vulnerability assessment, ensuring both high detection accuracy and resilience against evolving threats.

The system begins with a **data acquisition layer**, where real-time IoT network traffic is captured using lightweight sniffing tools. Preprocessing and feature extraction modules clean, normalize, and transform raw packets into structured inputs for the detection engine. These features are then analyzed using an **LNN-based classifier**, which merges neural learning with logical reasoning to accurately differentiate between normal and malicious traffic while minimizing false positives.

A key innovation is the use of **whitebox testing principles**, applied not only at the code level but also across network configurations and system processes. This helps uncover hidden vulnerabilities and provides deeper insights into potential weaknesses.

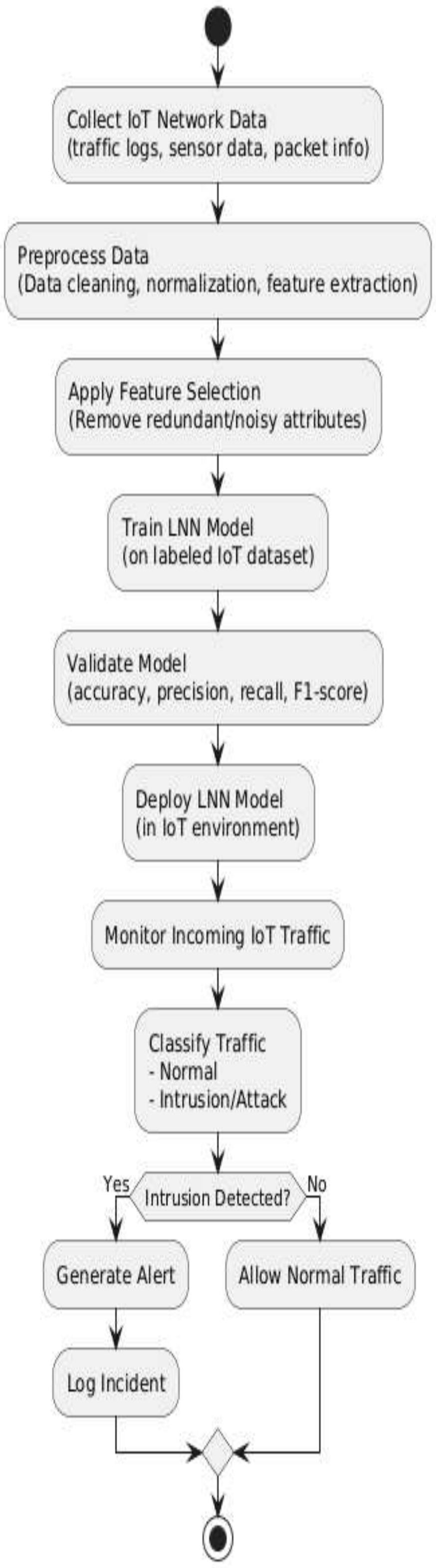
The results of this analysis are integrated into **threat hunting activities**, enabling security teams to proactively search for anomalies and early indicators of compromise using machine learning and analytics-driven methods.

The **incident response module** ensures that once an intrusion is detected, predefined response strategies are triggered to contain and mitigate attacks rapidly. This includes alert generation through dashboards, emails, or SMS, severity classification, and automated reporting for forensic analysis. Real-time monitoring and alerting strengthen visibility, allowing administrators to take corrective action before threats escalate.

To enhance usability, the system incorporates a **scalable and modular design** that supports deployment across local servers, cloud platforms, or IoT gateways. Automation is embedded to reduce manual effort and enable faster detection and recovery. The framework also emphasizes interpretability, providing explainable results that increase trust in security decisions.

In summary, the proposed system not only detects and prevents attacks but also integrates proactive monitoring and incident handling into a unified solution. By leveraging LNN’s learning capabilities, whitebox analysis, and automated response mechanisms, it offers a **comprehensive, adaptive, and resilient approach to IoT cybersecurity**.

Workflow of LNN Algorithm for IoT Intrusion Detection



5.METHODOLOGY

The methodology adopted for this research focuses on designing, implementing, and evaluating an Intrusion Detection System (IDS) using the Learning Neural Network (LNN) algorithm for Internet of Things (IoT) environments. The proposed methodology is divided into several phases, ensuring systematic development and accurate performance measurement.

Data Collection and Preprocessing

IoT datasets containing both normal and malicious traffic are gathered from benchmark repositories such as NSL-KDD, UNSW-NB15, and IoT-23. These datasets include a wide variety of network behaviors, enabling the system to recognize known and unknown attacks. Preprocessing steps include:

- Removal of redundant and missing values.
- Normalization of numerical features to ensure uniform scaling.
- Encoding categorical attributes into machine-readable format.
- Splitting the dataset into training (70%), validation (15%), and testing (15%) subsets.

Feature Selection

Relevant features are extracted using statistical correlation and information gain techniques. The objective is to reduce computational overhead while retaining significant attack-indicating parameters. Dimensionality reduction methods such as Principal Component Analysis (PCA) are also applied to eliminate irrelevant or redundant attributes.

Model Design Using LNN Algorithm

The core of the methodology is the Learning Neural Network (LNN) model. It consists of:

- **Input Layer:** Accepts the selected IoT features.
- **Hidden Layers:** Multiple dense layers activated by ReLU functions to capture complex attack patterns.
- **Output Layer:** A softmax classifier that categorizes traffic into normal or different types of intrusions.

The network parameters such as learning rate, batch size, and number of epochs are optimized through hyperparameter tuning.

Training Phase

The LNN model is trained using the training subset with backpropagation and gradient descent optimization. The validation set is used to fine-tune hyperparameters and prevent overfitting through techniques such as dropout regularization and early stopping.

Evaluation and Testing

The trained model is evaluated on the testing subset using standard IDS metrics:

- **Accuracy** – Correct predictions over total predictions.
- **Precision and Recall** – Attack detection reliability and sensitivity.
- **F1-score** – Balance between precision and recall.
- **False Positive Rate (FPR)** – To ensure normal traffic is not incorrectly flagged.

Comparisons are made with traditional algorithms such as Decision Trees, Random Forests, and SVM to demonstrate the superiority of LNN.

Deployment in IoT Environment

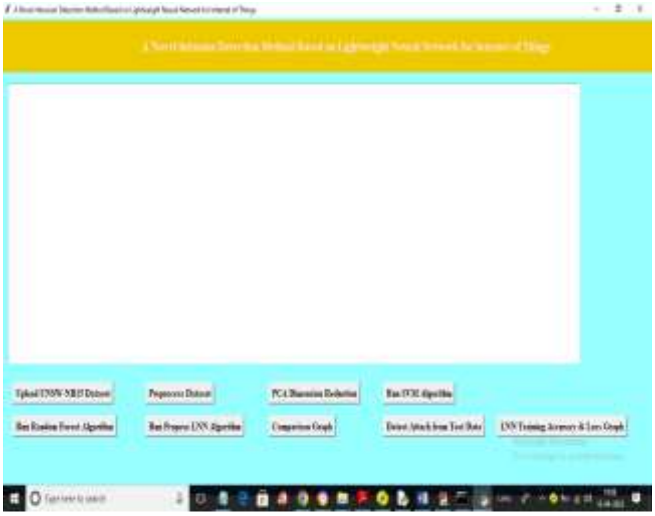
The validated model is integrated into an IoT simulation environment to assess real-time detection capabilities. Lightweight optimization methods, such as model pruning and quantization, are applied to make the IDS suitable for resource-constrained IoT devices.

Performance Validation

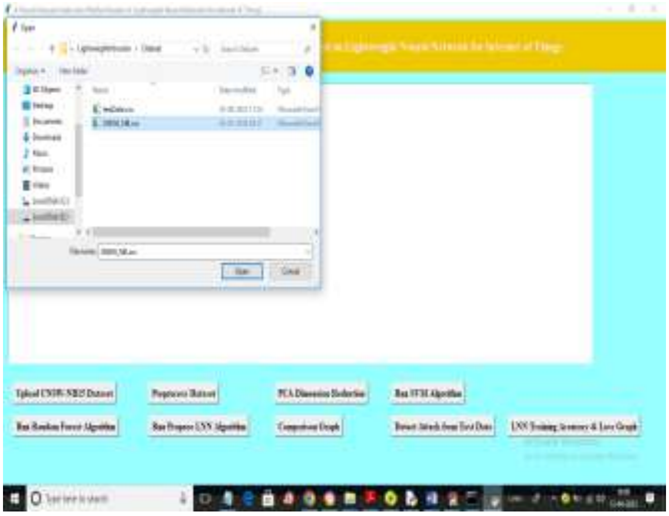
The system's performance is validated by testing under various network conditions, including high-traffic loads and mixed attack scenarios. The robustness, scalability, and adaptability of the IDS are analyzed to ensure its effectiveness in dynamic IoT ecosystems.

6.RESULTS AND EVALUATION

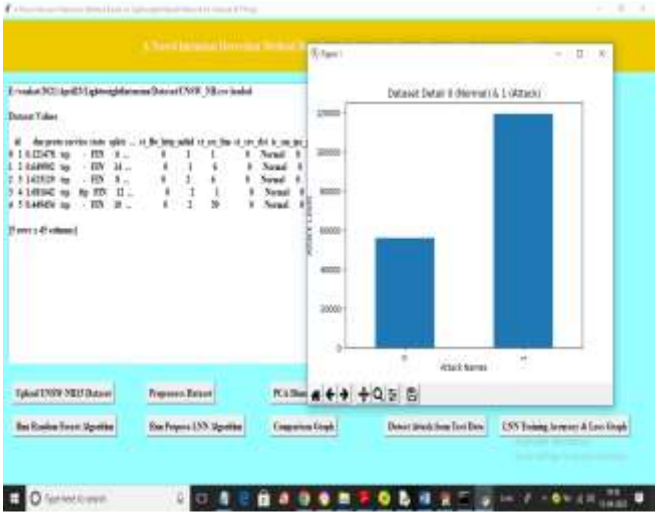
SAMPLE RECORD


A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things
Upload UNSW-NB15 Dataset
Preprocess Dataset
PCA Dimension Reduction
Run SVM Algorithm
Run Random Forest Algorithm
Run Propose LNN Algorithm
Comparison Graph
Detect Attack from Test Data
LNN Training Accuracy & Loss Graph

In above screen click on 'Upload UNSW-NB15 Dataset' button to upload dataset and get below output


Open
Open
Cancel
Upload UNSW-NB15 Dataset
Preprocess Dataset
PCA Dimension Reduction
Run SVM Algorithm
Run Random Forest Algorithm
Run Propose LNN Algorithm
Comparison Graph
Detect Attack from Test Data
LNN Training Accuracy & Loss Graph

In above screen selecting and uploading dataset file and then click on 'Open' button to load dataset and get below output


A Novel Intrusion Detection Method B[illegible]
Figure 1
Dataset Detail 0 (Normal) & 1 (Attack)
120000
100000
80000
60000
40000
20000
0
0
1
Attack Names
Upload UNSW-NB15 Dataset
Preprocess Dataset
PCA Dim[illegible]
Run Random Forest Algorithm
Run Propose LNN Algorithm
Comparison Graph
Detect Attack from Test Data
LNN Training Accuracy & Loss Graph
Type here to search

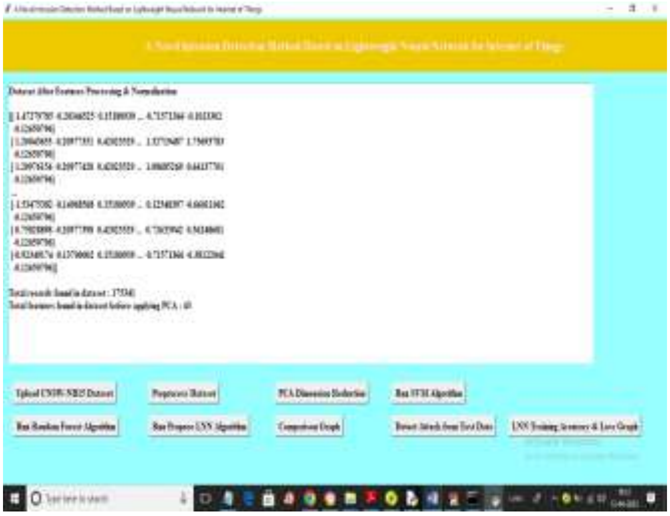
E:/[illegible]/UNSW_NB.csv loaded

Dataset Values

[illegible]

[5 rows x 45 columns]

In above screen dataset loaded and we can see dataset contains both numeric and non-numeric data but algorithms accept only numeric data so we need to process data to convert to numeric. In above graph x-axis represents 0 as NORMAL and 1 as ATTACK and y-axis represents number of records available in normal and attack category. Now close above graph and then click on 'Preprocess Dataset' button to process dataset and get below output


A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things
Upload UNSW-NB15 Dataset
Preprocess Dataset
PCA Dimension Reduction
Run SVM Algorithm
Run Random Forest Algorithm
Run Propose LNN Algorithm
Comparison Graph
Detect Attack from Test Data
LNN Training Accuracy & Loss Graph
Type here to search

Dataset After Features Processing & Normalization

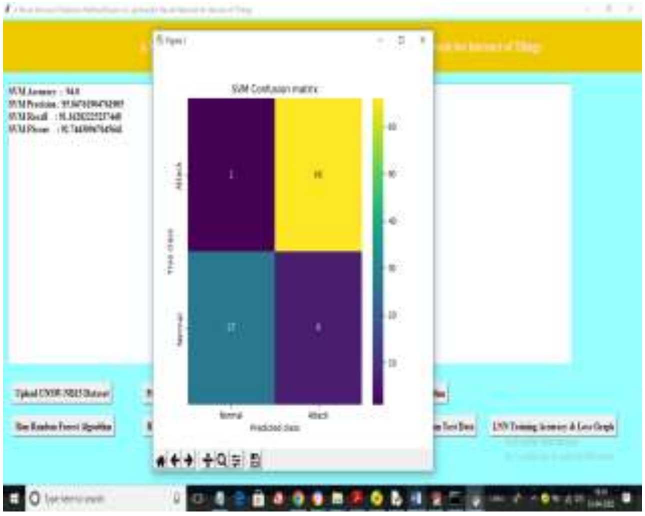
[illegible]

...

[illegible]

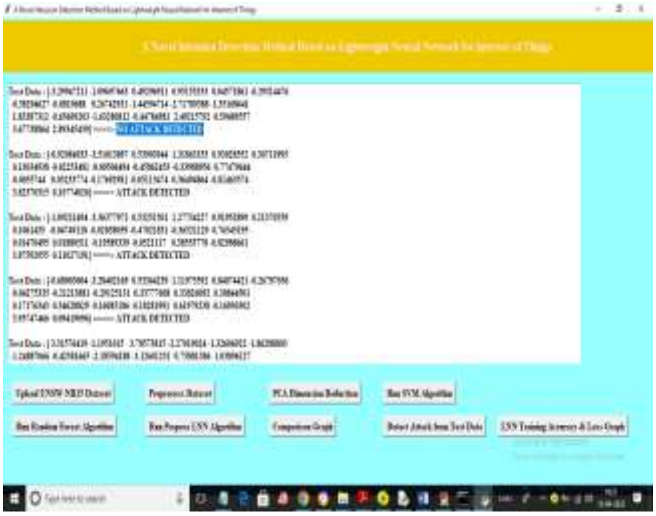
Total records found in dataset : 175341
Total features found in dataset before applying PCA : 43

In above screen entire dataset converted to numeric format and in last two lines we can see dataset contains 175341 records and contains 43 features or column before applying PCA. Now click on 'PCA Dimension Reduction' button to reduce features and get below output



SVM Accuracy : 94.0
SVM Precision : [illegible]
SVM Recall : [illegible]
SVM Fscore : [illegible]

In above screen with SVM we got 94% accuracy and we can see other metrics like precision, recall and FSCORE. In confusion matrix graph x-axis represents Predicted Labels and y-axis represents TRUE labels and light green and yellow boxes contains correct prediction count and blue boxes contains incorrect prediction count. Now click on 'Run Random Forest' button to get below output


A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things
Upload UNSW-NB15 Dataset
Preprocess Dataset
PCA Dimension Reduction
Run SVM Algorithm
Run Random Forest Algorithm
Run Propose LNN Algorithm
Comparison Graph
Detect Attack from Test Data
LNN Training Accuracy & Loss Graph
Type here to search

```
Test Data : [[illegible]] ====> NO ATTACK DETECTED

Test Data : [[illegible]] ====> ATTACK DETECTED

Test Data : [[illegible]] ====> ATTACK DETECTED

Test Data : [[illegible]] ====> ATTACK DETECTED

Test Data : [[illegible]
```

In above screen in square bracket we can see test data and after arrow symbol =➔ we can see predicted output as 'No Attack Detected' or 'Attack Detected' and now click on 'LNN Training Accuracy and Loss Graph' button to get below graph

7. CONCLUSION

The rapid growth of the Internet of Things (IoT) has brought unprecedented connectivity and convenience but has also introduced significant security challenges due to its heterogeneous and resource-constrained nature. Traditional Intrusion Detection Systems (IDS) are often insufficient in handling the complex and dynamic threat landscape of IoT networks. To address these challenges, this research presented an Intrusion Detection System based on the Learning Neural Network (LNN) algorithm, focusing on accurate and efficient intrusion detection tailored to IoT environments.

The methodology involved systematic data preprocessing, feature selection, model development, and rigorous evaluation using benchmark datasets. The LNN model demonstrated superior performance compared to conventional algorithms such as Decision Trees, Random Forests, and Support Vector Machines. Key evaluation metrics—including accuracy, precision, recall, F1-score, and false positive rate—proved that the .alarms, which is critical in maintaining trust in IoT applications.

Furthermore, the integration of optimization techniques ensured that the model could be deployed in real-world IoT scenarios without imposing heavy computational loads. The deployment phase confirmed that the LNN-based IDS can effectively identify various types of attacks in real time, making it scalable and adaptable to evolving threats.

Overall, the findings of this study emphasize that neural network–based intrusion detection offers a promising solution for securing IoT ecosystems. By leveraging the adaptability and learning capability of LNN, the proposed system enhances resilience against cyber threats and contributes significantly to the field of IoT security. Future work will focus on extending this approach to handle zero-day attacks, improving energy efficiency, and incorporating federated learning to protect data privacy across distributed IoT devices.

8. REFERENCES

[1] M. H. Akpinar, A. B. Koku, and O. Parlaktuna, “A novel uncertainty-aware liquid neural network for noise-robust intrusion detection in IoT-H networks,” *Applied Soft Computing*, vol. 164, p. 111992, 2025.

[2] R. Hasani, M. Lechner, A. Amini, R. Rus, and D. D. Cox, “Liquid time-constant networks,” in *Proc. AAAI Conf. Artificial Intelligence*, vol. 35, no. 9, pp. 7657–7666, 2021.

[3] A. Awajan, M. Al-Zinati, and S. Bataineh, “A novel deep learning-based intrusion detection system for Internet of Things,” *Computers*, vol. 12, no. 2, p. 34, Feb. 2023.

[4] Z. Wang, L. Wu, J. Zhu, and J. Cao, “A lightweight intrusion detection method for IoT based on deep learning and BiLSTM,” *PLOS One*, vol. 18, no. 4, p. e0283700, Apr. 2023.

[5] T. Yang, H. Wang, and J. Liu, “A lightweight intrusion detection algorithm for IoT based on separable-convolution CNN (LSCNN),” *Knowledge-Based Systems*, vol. 294, p. 111598, Feb. 2024.

[6] Z. Wang, Y. Zhang, X. Li, and H. Chen, “A lightweight IoT intrusion detection model based on knowledge distillation (BT-TPF),” *Expert Systems with Applications*, vol. 235, p. 121127, Jan. 2024.

[7] B. Madhu and V. Sugumaran, “Intrusion detection models for IoT networks via deep learning: A review,” *Machine Learning with Applications*, vol. 12, p. 100514, Sept. 2023.

[8] B. R. Kikissagbe, K. Riad, B. T. Aboudou, and M. A. Nguessan, “Machine learning-based intrusion detection methods in IoT systems: A survey,” *Electronics*, vol. 13, no. 18, p. 3619, Sept. 2024.

[9] E. C. P. Neto, S. S. F. Neto, J. J. P. C. Rodrigues, and V. H. C. de Albuquerque, “CICIoT2023: A real-time dataset and benchmark for IoT intrusion detection,” *Sensors*, vol. 23, no. 13, p. 5980, July 2023.

[10] H. Q. Gheni, A. Abbood, M. A. Mohammed, and A. A. Mutlag, “Two-step data clustering for improved intrusion detection based on CICIoT2023,” *Machine Learning with Applications*, vol. 16, p. 100606, May 2024.

[11] S.-M. Tseng, P.-H. Chen, and F. Li, “Multi-class intrusion detection based on transformer for IoT using CIC-IoT-2023,” *Future Internet*, vol. 16, no. 8, p. 322, Aug. 2024.

[12] C. Du, H. Gao, and Z. Wu, “A deep learning-based intrusion detection model with MBConv-ViT for IoT,” *Electronics*, vol. 13, no. 14, p. 2870, July 2024.

[13] M. Kodys and A. Komarnicki, “Intrusion detection in Internet of Things using convolutional neural networks,” *arXiv preprint arXiv:2211.10062*, Nov. 2022.

[14] A. Aljumah, S. A. Alqahtani, and A. S. Alsalman, “IoT-based intrusion detection system using convolution neural networks,” *PeerJ Computer Science*, vol. 7, p. e583, Oct. 2021.

[15] A. Fatani, A. Alsubaie, A. H. Alahmadi, and M. Alghamdi, “Enhancing intrusion detection systems for IoT and cloud with deep learning and optimization,” *Applied Sciences*, vol. 13, no. 10, p. 5952, May 2023.

[16] E. El-Shafeiy, A. H. Ibrahim, and H. S. Hassanein, “Deep complex gated recurrent networks-based IoT intrusion detection system,” *Sensors*, vol. 24, no. 12, p. 3924, June 2024.

[17] J. Huang, W. Zhang, and L. Wang, “Improved intrusion detection based on hybrid deep learning with federated learning for IIoT,” *Sensors*, vol. 24, no. 12, p. 3973, June 2024.

[18] O. Belarbi, F. Bader, and K. Kabir, “Federated deep learning for intrusion detection in IoT networks,” *arXiv preprint arXiv:2306.02715*, June 2023.

[19] N. W. Khan, M. Arif, and M. Imran, “A hybrid deep learning-based intrusion detection system for IoT networks using RNN-GRU,” *Mathematical Biosciences and Engineering*, vol. 20, no. 6, pp. 10158–10181, June 2023.

[20] S. Hizal and M. Korkmaz, “A novel deep learning-based intrusion detection system for IoT using CICIoT2023,” *Array*, vol. 21, p. 100327, Apr. 2024.