DL-IDF:A Resilient Deep Leaning Methodology for Securing Industrial IOT Networks

Ms. N Sravani
UG Student, Dept of CSE,
CMR Technical Campus
Hyderabad, Telangana, India
237r1a05w7@cmrtc.ac.in

K. Sai Charan
UG Student, Dept of CSE,
CMR Technical Campus
Hyderabad, Telangana, India
247r5a0530@cmrtc.ac.in

S Moksha Netra
UG Student, Dept of CSE,
CMR Technical Campus
Hyderabad, Telangana,
India
237r1a05y2@cmrtc.ac.in

G Pavan Kumar
Assistant Professor,
Dept of CSE, CMR Technical
Campus Hyderabad,
Telangana, India
pavankumar.cse@cmrtc.ac.in

G Swarnalatha
Assistant Professor,
Dept of CSE, CMR Technical
Campus Hyderabad,
Telangana, India
gswarnalatha.cse@cmrtc.ac.in

How to Cite this Article:

Sravani, N., Charan, K. S. & Netra, S. M. (2026). DL-IDF:A Resilient Deep Leaning Methodology for Securing Industrial IOT Networks. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.366

https://doi.org/10.55041/ijcope.v2i4.366

ABSTRACT— Industrial Internet of Things (IoT) is widely recognized field that allows to connect all devices. It works in a process of gathering data, data exchange, and runs automatically. It mainly involves automation tasking without any human intervention, which results high efficiency and less amount of costs. However, IoT results for good monitoring and tracking real-time insights, it also has the cons that make IoT in high danger that leads to cyber-attacks as the devices are interconnected. To overcome this issue, we present a deep learning- based hybrid framework integrating Deep Neural Networks (DNN) with Extreme Learning Machine (ELM) to make Internet of Things more secure. In this proposed system we analyze data by extracting a NSL-KDD dataset which is trained to resolve the duplication of data and uneven distribution of data issues present in the previous intrusion detection dataset and present the accuracy of each model. To address security risks like cyber-attacks, a hybrid deep learning model using DNN and ELM is proposed to enhance intrusion detection and ensure more secure IoT systems.

INTRODUCTION

Industrial Internet of Things (IIoT) has emerged as a key technology in modern digital systems, enabling seamless connectivity between devices, sensors, and networks. It allows real-time data collection, monitoring, and automation across various industries, improving efficiency and reducing operational costs. However, the increasing number of interconnected devices also introduces significant security challenges. Traditional network security mechanisms struggle to detect evolving cyber threats, especially in large-scale and dynamic IoT environments. These systems often rely on static rules or signature-based detection, making them ineffective against unknown or sophisticated attacks.

Intrusion Detection Systems (IDS) play a crucial role in identifying malicious activities within a network. Conventional IDS approaches, including machine learning models such as Support Vector Machines and Random Forest, face limitations in handling high-dimensional data, detecting rare attacks, and maintaining accuracy across diverse datasets. Additionally, issues such as data imbalance and high false positive rates further reduce their effectiveness in real-world scenarios.

To overcome these limitations, deep learning techniques offer a more adaptive and intelligent approach to intrusion detection. In particular, Deep Neural Networks (DNN) can learn complex patterns from network traffic data, while Extreme Learning Machine (ELM) provides faster training and efficient generalization. By integrating DNN with ELM, a hybrid model can leverage the strengths of both techniques to improve detection accuracy and processing speed.

In this project, a hybrid intrusion detection framework is developed using DNN and ELM, trained on the NSL-KDD dataset. The system performs data preprocessing, feature selection, and classification to accurately identify cyber-attacks in IoT environments. This approach enhances the security of interconnected systems by enabling real-time threat detection, reducing false positives, and providing a scalable solution for modern network security challenges.

I. PROBLEM DEFINITION

Industrial Internet of Things (IoT) networks enable communication between a large number of interconnected devices, making systems more efficient and automated. However, this connectivity also introduces serious security challenges, as IoT environments are highly vulnerable to cyber-attacks such as denial-of-service, probing, and unauthorized access. The large volume and dynamic nature of network traffic make it difficult to monitor and detect malicious activities effectively using traditional security approaches.

Conventional Intrusion Detection Systems (IDS), which rely on signature-based methods or basic machine learning algorithms, are often unable to detect unknown or evolving threats. These systems suffer from limitations such as low detection accuracy, high false positive rates, and poor performance when handling imbalanced datasets. Additionally, many existing methods struggle to process large-scale real-time data, reducing their effectiveness in modern IoT environments.

Therefore, there is a need for an advanced and efficient intrusion detection system that can accurately identify both known and unknown attacks while handling complex and high-dimensional data. This project addresses these challenges by proposing a hybrid deep learning-based IDS using Deep Neural Networks (DNN) and Extreme Learning Machine (ELM), which improves detection accuracy, reduces false alarms, and enhances overall security in IoT networks.

1.2 PROJECT FEATURES

The proposed Intrusion Detection System includes advanced features that enhance security in Industrial IoT environments by accurately detecting cyber threats using a hybrid deep learning approach. It combines Deep Neural Networks (DNN) for capturing complex patterns and Extreme Learning Machine (ELM) for faster processing, resulting in improved accuracy and reduced detection time. The system applies data preprocessing techniques such as feature selection, label encoding, and normalization to improve performance and eliminate redundant data. It is capable of handling large-scale and real-time network traffic while reducing false positives and detecting both known and unknown attacks. Additionally, it supports both network-based and host-based intrusion detection, provides detailed performance evaluation using metrics like accuracy, precision, recall, and F1-score, and offers a scalable, lightweight, and cost-effective solution for securing IoT networks.

Related Work

Several research studies have explored the use of machine learning and deep learning techniques to improve intrusion detection in network security. Traditional approaches include signature-based detection methods, statistical analysis, and classical machine learning algorithms such as Support Vector Machines and Random Forest. While

these methods provide a certain level of protection, they often fail to detect unknown or evolving cyber threats and may produce high false positive rates.

Recent research has focused on deep learning models for intrusion detection, including Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN). These approaches are capable of learning complex patterns from large-scale network traffic data and improving detection accuracy. Datasets such as NSL-KDD have been widely used to evaluate these models, addressing some limitations of earlier datasets like redundancy and imbalance.

However, many existing solutions face challenges such as high computational complexity, slow training time, and difficulty in handling imbalanced data. Some models also lack the ability to generalize across different types of attacks or real-time environments. This project builds upon existing research by proposing a hybrid model that integrates Deep Neural Networks with Extreme Learning Machine (ELM), providing faster processing, improved accuracy, and a more efficient solution for intrusion detection in IoT networks.

II. METHODOLOGY

1. Data Collection

NSL-KDD dataset is used, containing normal and attack network traffic data.

2. Data Preprocessing

Data is cleaned, encoded, normalized using MinMax scaling, and split into training and testing sets.

3. Feature Selection

Important features are selected using Pearson correlation and Chi-square methods, and irrelevant features are removed.

4. Model Training

A hybrid model using DNN and ELM is trained to learn patterns in network traffic.

5. Classification & Evaluation

The model classifies traffic as normal or attack and is evaluated using accuracy, precision, recall, F1-score, and confusion matrix.

III. PROPOSED SYSTEM

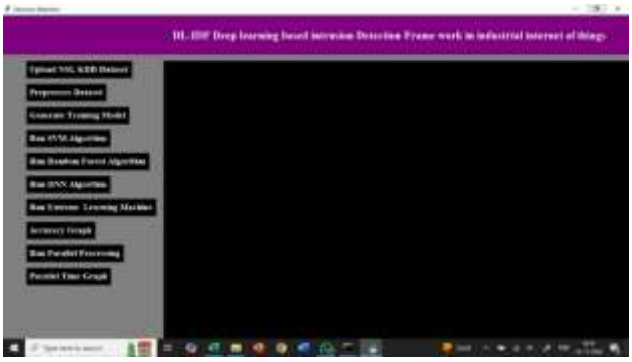
The proposed system uses a hybrid deep learning approach for intrusion detection in Industrial IoT networks by combining Deep Neural Networks (DNN) and Extreme Learning Machine (ELM). It analyzes network traffic using the NSL-KDD dataset to identify both normal and malicious activities. DNN is used to learn complex patterns in the data, while ELM enables faster training and efficient classification. The system includes preprocessing and feature selection techniques to handle large, imbalanced datasets and improve performance. Compared to traditional methods, it reduces false positives and increases detection accuracy for both known and unknown attacks, providing a scalable and efficient solution for real-time network security in IoT environments.

IV. IMPLEMENTATION DETAILS

The implementation of the proposed intrusion detection system is carried out using both frontend and backend technologies along with machine learning integration. The frontend is developed using HTML, CSS, and JavaScript to provide a simple and user-friendly interface for displaying results and system outputs. The backend is implemented using Python to handle data preprocessing, model training, and real-time intrusion detection using the hybrid DNN and ELM approach. The system uses the NSL-KDD dataset for training and testing the model. It allows users to input or process network traffic data, classify it as normal or malicious, and view detection results through an interactive interface.

4.1 ALGORITHMS USED

4.1.1 DEEP NEURAL NETWORK (DNN)



Deep Neural Network (DNN) is a deep learning algorithm used to learn complex patterns from large datasets. It consists of multiple hidden layers that help in extracting high-level features from network traffic data. In this project, DNN is used to classify network connections as normal or malicious by learning hidden relationships in the NSL-KDD dataset. It improves detection accuracy by handling non-linear and complex data patterns effectively.

4.1.2 EXTREME LEARNING MACHINE (ELM)

Extreme Learning Machine (ELM) is a fast-learning algorithm used for single hidden layer neural networks. It randomly assigns input weights and computes output weights analytically, making the training process very fast. In this project, ELM is used for efficient classification of intrusion data, reducing training time while maintaining good accuracy. It is particularly useful for large-scale IoT datasets.

4.1.3 SUPPORT VECTOR MACHINE (SVM)

Support Vector Machine (SVM) is a supervised machine learning algorithm used for classification tasks. It works by finding an optimal hyperplane that separates different classes. In this project, SVM is used as a baseline model to compare performance with deep learning approaches in detecting network intrusions.

4.1.4 RANDOM FOREST (RF)

Random Forest is an ensemble learning algorithm that builds multiple decision trees and combines their outputs for final prediction. It helps improve accuracy and reduce overfitting. In this project, it is used to classify network traffic and compare results with deep learning-based models.

V. EXPERIMENTAL RESULTS AND DISCUSSION

The following screenshots represent the execution and performance of the proposed Intrusion Detection System. These figures demonstrate the working of different modules such as data preprocessing, feature selection, model training, and intrusion classification. The results clearly show how the system identifies normal and malicious network traffic using the hybrid DNN and ELM approach. It also highlights the effectiveness of the system in improving detection accuracy, reducing false positives, and ensuring secure and reliable monitoring of IoT network traffic.

System Interface – Home Page:

The above figure shows the main interface of the system where users can perform all algorithms to know the accuracy.

Fig. 1. Home UserInterface

In this figure, the user uploads a dataset to the system.

Fig. 2. Final Output Page

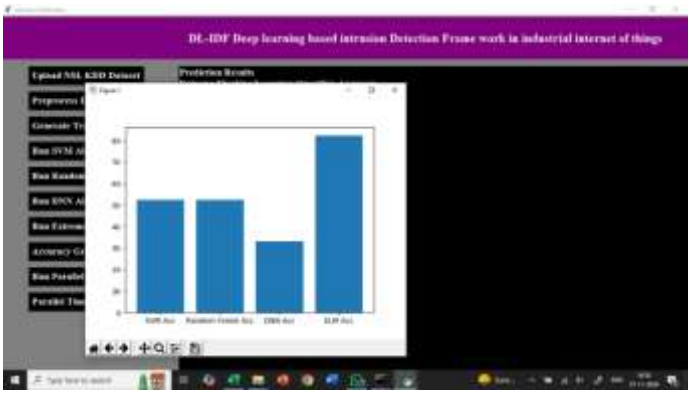


Fig. 3. Accuracy Graph

Fig 3: gives the accuracy graph comparison which gives us a pictorial representation and easy understandable way just by looking into the graph. The SVM algorithm consists accuracy of 52.3% as it is very slow in taking larger datasets. The Random Forest has an accuracy of same 52.3% due to it cannot overfit noisy data and sometimes it produces less interpretability results. The DNN algorithm consists of low accuracy consisting of just 33.2% because it needs large amounts of data and computational resources.

VI. CONCLUSION

This project presents an efficient intrusion detection system for Industrial IoT networks using a hybrid approach that combines Deep Neural Networks (DNN) and Extreme Learning Machine (ELM). The system effectively addresses challenges in traditional intrusion detection methods such as low accuracy, high false positive rates, and inability to detect evolving cyber-attacks. By using the NSL-KDD dataset along with preprocessing and feature selection techniques, the model improves detection performance for both known and unknown attacks. The integration of DNN and ELM enhances learning capability, reduces training time, and

provides better scalability. Overall, the proposed system offers a reliable and effective solution for real-time intrusion detection in modern IoT environments.

VII. FUTURE SCOPE

The proposed intrusion detection system can be further enhanced by integrating advanced deep learning techniques for real-time threat detection and predictive analysis. Future improvements may include the use of more powerful architectures such as CNN, RNN, or LSTM to better capture complex and sequential patterns in network traffic. The system can also be optimized to handle large-scale IoT environments more efficiently and improve detection performance on imbalanced datasets. Additionally, integrating real-time monitoring and automated response mechanisms can help in instantly mitigating detected attacks. These enhancements will make the system more accurate, scalable, and suitable for real-world cybersecurity applications.

VIII.ACKNOWLEDGMENT

We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project, we take this opportunity to express our profound gratitude and deep regard to our guide **G PAVAN KUMAR** Designation for his/her exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by him/her shall carry us a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to the Project Review Committee (PRC) coordinators **G SWARNALATHA** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **N.BHASKAR** Head, Department of Computer Science and Engineering for providing encouragement and support for completing this project successfully.

We are deeply grateful to **Dr. A. Raji Reddy**, Director, for his cooperation throughout the course of this project. Additionally, we extend our profound gratitude to **Sri. Ch. Gopal Reddy**, Chairman, **Smt. C. Vasantha Latha**, Secretary and **Sri. C. Abhinav Reddy**, Vice-Chairman, for fostering an excellent infrastructure and a conducive learning environment that greatly contributed to our progress.

The guidance and support received from all the members of CMR Technical Campus who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

IX. REFERENCES

[1] Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). *Network Intrusion Detection*. IEEE Network, 8(3), 26–41.

[2] Staudemeyer, R. C. (2015). *Applying Long Short-Term Memory Recurrent Neural Networks to Intrusion Detection*. South African Computer Journal, 56(1), 136–154.

[3] Vinayakumar, R., Alazab, M., Soman, K. P., & Poornachandran, P. (2019). *Deep Learning Approach for Intelligent Intrusion Detection System*. IEEE Access.

[4] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). *A Deep Learning Approach to Network Intrusion Detection*. IEEE Transactions on Emerging Topics in Computational Intelligence.

[5] Moustafa, N., & Slay, J. (2015). *The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Dataset*. IEEE.

[6] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). *A Detailed Analysis of the KDD CUP 99 Data Set*. IEEE Symposium on Computational Intelligence for Security and Defense Applications.