International Journal of Engineering in Computer Science

E-ISSN: 2663-3590
P-ISSN: 2663-3582
Impact Factor (RJIF): 5.52
www.computersciencejournals.com/ijecs
IJECS 2025; 7(2): 117-126
Received: 02-07-2025
Accepted: 25-07-2025

Nisha
Associate Professor,
Department of Computer Science, Govt. P. G. College for Women, Rohtak, Haryana, India

Corresponding Author:
Nisha
Associate Professor,
Department of Computer Science, Govt. P. G. College for Women, Rohtak, Haryana, India

Deep learning based threat detection framework for cyber security applications

Nisha

DOI: https://www.doi.org/10.33545/26633582.2025.v7.i2b.206

Abstract

This study presents a deep learning-based threat detection framework for cybersecurity applications, focusing on accurately identifying malicious network activity. The methodology begins with the collection of network traffic data using the CICIDS2017 dataset, which includes realistic benign traffic and contemporary attack scenarios, addressing limitations of previous datasets such as insufficient diversity and incomplete metadata. Pre-processing ensures high-quality data by removing noise, handling missing values, encoding categorical features, normalizing numerical attributes, and addressing class imbalances. Exploratory Data Analysis (EDA) is performed to uncover patterns, outliers, and feature correlations, guiding effective model selection. Both baseline machine learning models—Logistic Regression, Random Forest, and XG-Boost—and deep learning models, including a Fully Connected Feedforward Neural Network (FNN) and a 1D Convolutional Neural Network (1D-CNN), are implemented and evaluated. Comparative analysis shows that while classical models perform reasonably well, deep learning models, particularly the 1D-CNN, achieve superior performance, with an accuracy of 97.5%, high precision, recall, and AUC metrics. The results demonstrate the framework's ability to capture complex feature interactions and sequential patterns in network traffic, providing robust, reliable, and generalizable detection of cyber threats. This study highlights the effectiveness of deep learning approaches in enhancing real-world intrusion detection systems.

Keywords: Deep learning threat detection cybersecurity, intrusion detection system (ids), 1d convolutional neural network (1d-cnn)

Introduction

Cyber threats are one of the largest problems for people, businesses, and governments in the digital age. Devices that link to the internet, mobile technology, and cloud computing have all evolved extremely swiftly. This has made the attack surface much bigger, which means that traditional ways of protecting computers don't work as well. Traditional signature-based or rule-based detection systems frequently fail to recognize new, intricate, or zero-day attacks, hence rendering networks and systems vulnerable to breaches, data theft, or service disruptions. Adding artificial intelligence, especially deep learning, to cybersecurity frameworks is one way to get past these challenges. Deep learning is a type of machine learning that uses neural networks with several layers to find patterns or representations in large amounts of data. It works best in fast-paced, high-volume cyber situations because it can automatically find features and adjust to new threats. A lot of research over the last ten years has shown that deep learning models like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory networks (LSTMs), and Autoencoders can find malware, phishing attempts, and distributed denial-of-service (DDoS) attacks with a high level of accuracy [1, 2]. Employing these models helps find little patterns and connections that regular detection systems often miss, which improves an organization's security better as a whole. These are good things, but there are still problems with employing deep learning-based cybersecurity tools in the real world. There are a lot of problems with neural networks. They demand a lot of processing power, huge and varied training datasets, and they can be fooled by assaults from other networks, for example. It's also important to find a balance between how well risks are detected and how quickly they are found, since delays in finding threats might have big effects.

We need a complete system with deep learning models, good preprocessing, feature extraction, and ways to maintain learning in order to fix these problems. Security experts should be able to comprehend and adjust the system as new threats come up, therefore this kind of architecture should also have ways for models to be understood and changed. Things get much more complicated as more people use edge computing and Internet of Things (IoT) devices. This is because the different sorts and amounts of network traffic need detection systems that can expand and spread [3-5]. Deep learning frameworks can process a lot of cybersecurity data in real time because modern GPUs and cloud infrastructures can operate on many tasks at once. This helps them find and fix problems before they happen [6-9]. The system might also be able to generate better predictions and adapt if it uses deep learning with other technologies like natural language processing, reinforcement learning, and threat intelligence feeds. This plan covers everything and makes it easier to discover threats while also lowering the number of false positives. This helps businesses stay focused on what's most important and make better use of their resources. The cyber threat landscape is always changing, therefore it's important to build threat detection frameworks that are strong, smart, and easy to grow. This will keep businesses going, protect crucial information, and keep users' trust [10-12]. The goal of the proposed project is to provide a threat detection framework for cybersecurity applications that employs deep learning to get around present limitations, improve accuracy, and satisfy real-time operational objectives. This framework aims to safeguard digital infrastructures against a diverse array of cyber-attacks in a dependable, efficient, and sustainable manner by integrating sophisticated neural network architectures, optimal training techniques, and adaptive learning systems. If this kind of architecture succeeds, it might change the way cybersecurity is done by giving businesses a smart, proactive defense system that can respond to threats that are always changing [13, 14].

Literature Review

Tulsyan 2024 *et al*. looks into how well machine learning (ML) can uncover problems with cybersecurity. As cyber-attacks become more widespread and complicated, standard security measures may not be enough. This means we need better solutions that can be changed to fit different needs. This study evaluates various machine learning techniques, including supervised, unsupervised, and deep learning models, for detecting malware, phishing, and network intrusions, highlighting their benefits and limitations. Despite significant progress compared to conventional methods, challenges such as algorithmic bias, data quality, and responsiveness to emerging threats persist. looks at new trends and probable ways to incorporate ML to real-time cybersecurity systems in the future [15].

Roopesh 2024 *et al*. Cybersecurity is growing increasingly crucial as cyberattacks become more widespread and more difficult to stop. Machine learning (ML) and deep learning (DL) are becoming highly significant for improving security systems. They let you find threats, unusual behavior, and intrusions in real time. This systematic review, following PRISMA guidelines, looks at how machine learning (ML) and deep learning (DL) can be used to protect networks, clouds, and the Internet of Things (IoT). It shows how models like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) work better than traditional rule-based methods. It also talks about problems like adversarial attacks, data privacy, and high computation needs, and it offers solutions like adversarial training, federated learning, and model optimization to make things work better and keep them safe [16].

Maureen 2024 *et al*. Deep learning (DL) has greatly improved cybersecurity by allowing us to find and stop threats straight immediately. Convolutional and recurrent neural networks are very good at finding patterns and outliers in big, complicated data sets. This makes it easier to find phishing, malware, and insider threats. The system works better because these models learn on their own from network traffic, user activity, and system records. There are still problems, such adversarial attacks that take advantage of DL's weaknesses. This shows how important it is to have effective training, add more data, and do things like adversarial training to protect yourself. DL, together with regular security procedures and threat intelligence, can help you build powerful, flexible, and safe cyber infrastructures [17].

Srinivasan 2022 *et al*. Deep Learning (DL) is a sophisticated type of machine learning that is often used in cybersecurity since it works better than older ML methods. It goes into a lot of detail about the different DL architectures that have been used, are being used, and will be used in the future for a wide range of cybersecurity tasks, such as finding malware, botnets, spam, phishing, network traffic, binary analysis, insider threats, CAPTCHA, and steganography. It looks at how DL is used in a number of fields, including as the Internet of Things (IoT), cloud security, biometrics, encryption, and edge computing. The study discusses emerging requirements in smart cities, cyber-physical systems, and Industry 4.0. It talks about problems that still need to be fixed and gives ideas for new DL designs for future research [18].

Ghillani 2022 *et al*. looks into how deep learning (DL), which comes from artificial neural networks, might be used to improve cybersecurity in Industry 4.0 and cyber-physical systems (CPS). Deep learning (DL) methods including MLPs, CNNs, RNNs, LSTMs, autoencoders, and hybrid models make it possible to intelligently find malware, intrusions, botnet traffic, and IoT vulnerabilities. SGD, L-BFGS, and Adam are all training methods that improve network performance, however there are still problems like tweaking hyperparameters and high computational costs. Combining AI with CPS and IoT makes it possible to do real-time sensing, processing, and predictive cyber risk analytics, which helps make cyber infrastructures safe, strong, and adaptable in complex digital environments that are linked to each other [19].

Table 1: Literature Summary

Authors/year	Methodology	Research gap	Findings
Ashraf/2022 [20]	Ensemble-based intrusion detection methodology.	Limited adaptive, real-time intrusion detection using ensemble machine learning.	RFMLP ensemble model improves intrusion detection accuracy over existing approaches.
Karn/2021 [21]	Progressive learning algorithms applied for network threat detection analysis.	Limited exploration of progressive learning in cybersecurity domain.	Proposed metrics predict catastrophic forgetting, improving automated threat detection.
Abushark/2019 [22]	IntruDTree uses feature ranking and tree-based model construction.	Existing IDS lack feature selection and computational efficiency improvements.	IntruDTree outperforms traditional ML models in accuracy, precision, efficiency.
Ullah/2019 [23]	Combined deep learning detects software piracy and malware infections.	Limited studies address IoT security using dual deep-learning approaches.	Proposed model outperforms existing methods in IoT threat detection.
Narayanan/2018 [24]	Cognitive system integrates knowledge graph and machine learning agents.	Limited frameworks combine semantic reasoning with collaborative cybersecurity analysis.	Framework improves threat detection, reduces analyst workload, increases confidence.

Methodology

The study strategy involves systematically gathering and cleaning up network traffic data, then utilizing Exploratory Data Analysis (EDA) to find patterns and building machine learning and deep learning models. This method makes sure that threats are found accurately, models are optimized well, and real cybersecurity applications are thoroughly tested.

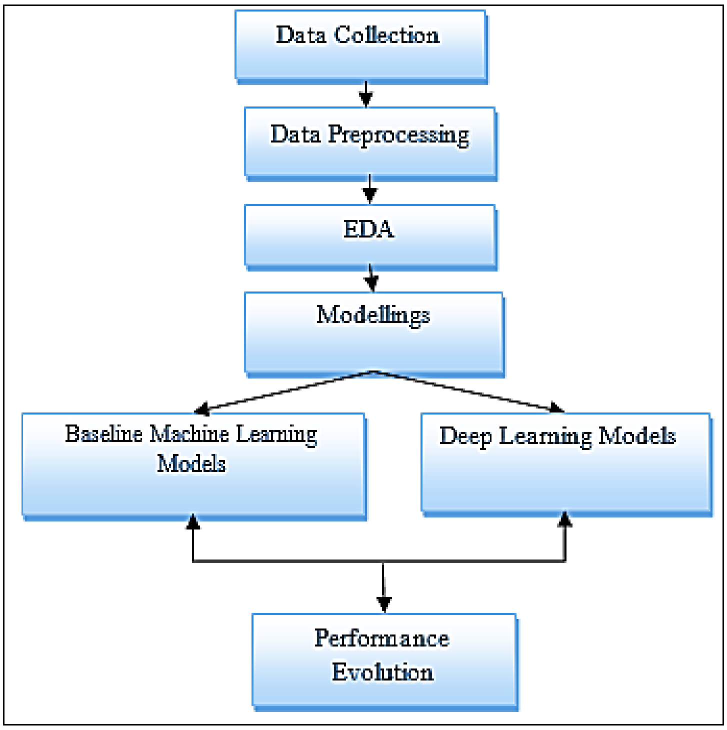


Fig 1: Proposed Flow Chart

A. Data Collection

Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) https://www.unb.ca/cic/datasets/ids-2017.html?utm_source=chatgpt.com are crucial for https://www.unb.ca/cic/datasets/ids 2017.html?utm_source=chatgpt.com defending against sophisticated network attacks. However, anomaly-based approaches often suffer from inconsistent performance due to outdated or unreliable datasets. Evaluations of eleven datasets since 1998 reveal issues such as limited traffic diversity, insufficient attack coverage, anonymized payloads, and missing metadata. The CICIDS2017 dataset addresses these gaps by including benign traffic and up-to-date common attacks, closely resembling real-world PCAPs. Using CICFlowMeter, flows are labeled with timestamps, IPs, ports, protocols, and attacks. Realistic background traffic was generated using the B-Profile system, modeling the behavior of 25 users across HTTP, HTTPS, FTP, SSH, and email protocols.

B. Data Pre-processing

Preprocessing makes sure that the data is of good quality and ready for training once it has been obtained. This means getting rid of noise, missing numbers, duplication, or features that aren't important. You need to standardize or encode numerical and categorical information. For example, you can use one-hot encoding for categorical variables. Feature selection methods can reduce dimensionality and improve model performance by maintaining only the most important information. You can also utilize SMOTE or data augmentation to fix problems with class imbalance.

Preprocessing makes ensuring that the data is well-organized, structured, and balanced. This creates a strong foundation for developing deep learning models that can discover trends and problems in cybersecurity datasets.

C. Exploratory Data Analysis (EDA)

Exploratory Data Analysis (EDA) lets you figure out how the data is set up and what patterns it has. The class distribution shows how many good and bad flows there are. This can highlight any class imbalance that could make it harder to train the model. The heatmap of feature correlation shows how the different sections of network traffic are linked to each other. This helps you locate features that are closely linked and choose which ones to use. Histograms of significant flow data show how essential features are spread out, which can show patterns, changes, and possible outliers. EDA helps you understand the dataset better by looking at these things. It also helps you make judgments about preprocessing and builds strong and reliable threat detection models.

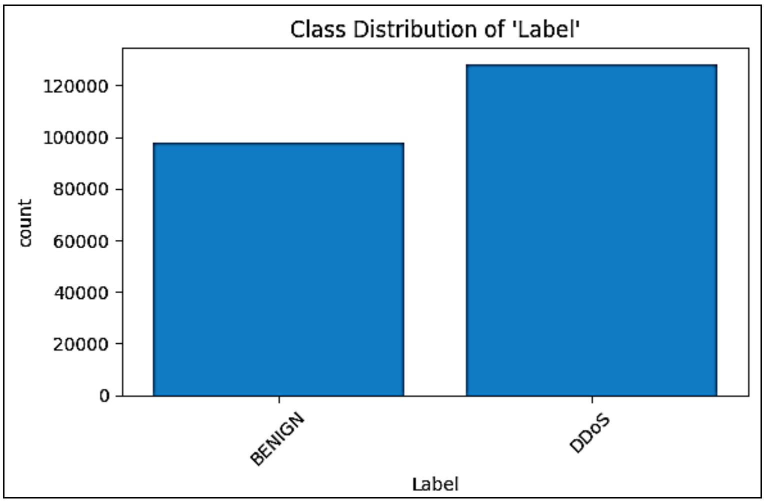


Fig 2: Class distribution

Fig. 2 shows the class distribution of the dataset, including the percentage of normal and attack cases. This helps plan model evaluation by showing class imbalance.

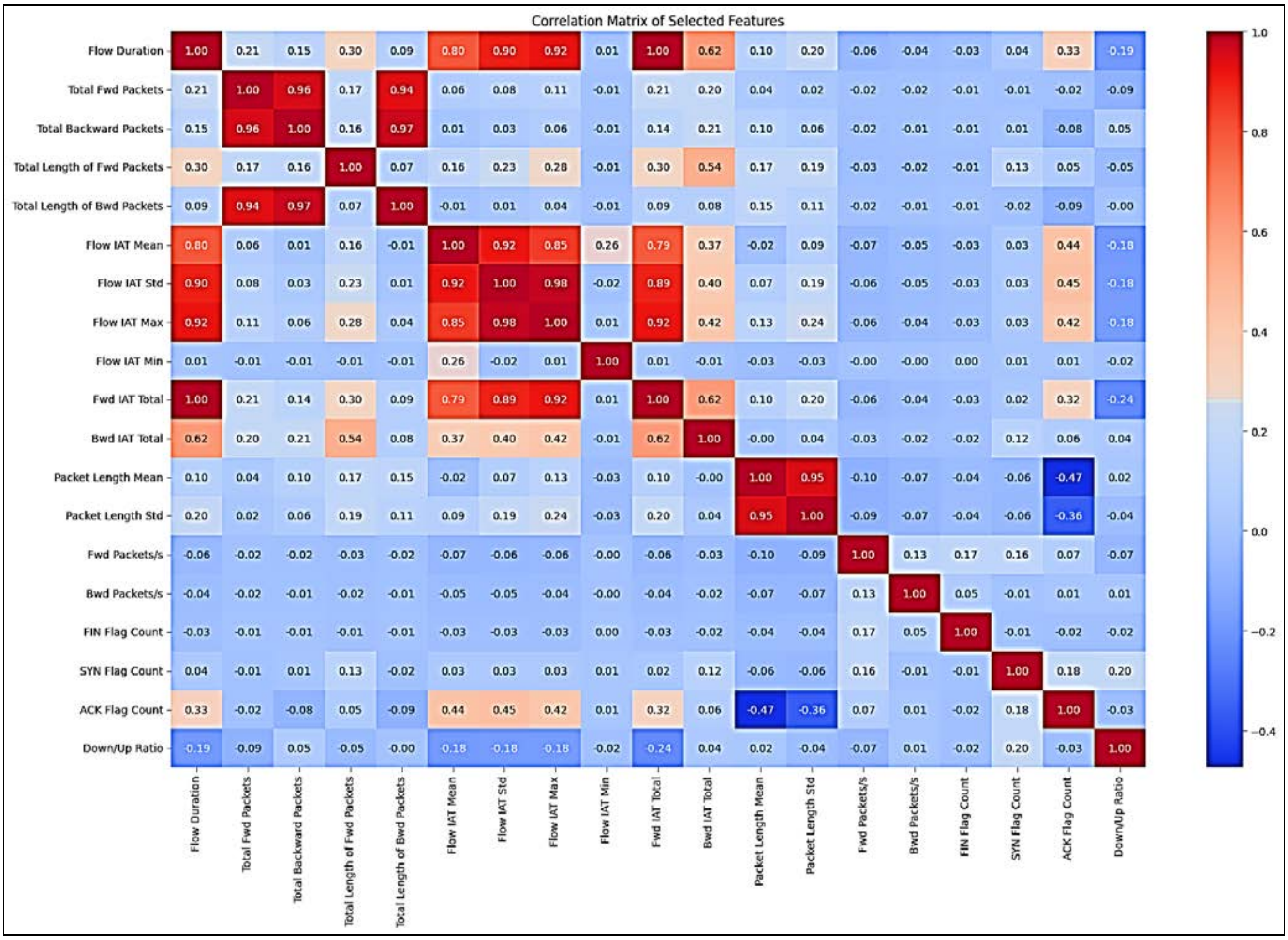


Fig 3: Feature correlation heatmap

Fig.3 shows a feature correlation heatmap, visualizing relationships between network traffic features, identifying strongly correlated attributes, and guiding feature selection and model optimization.

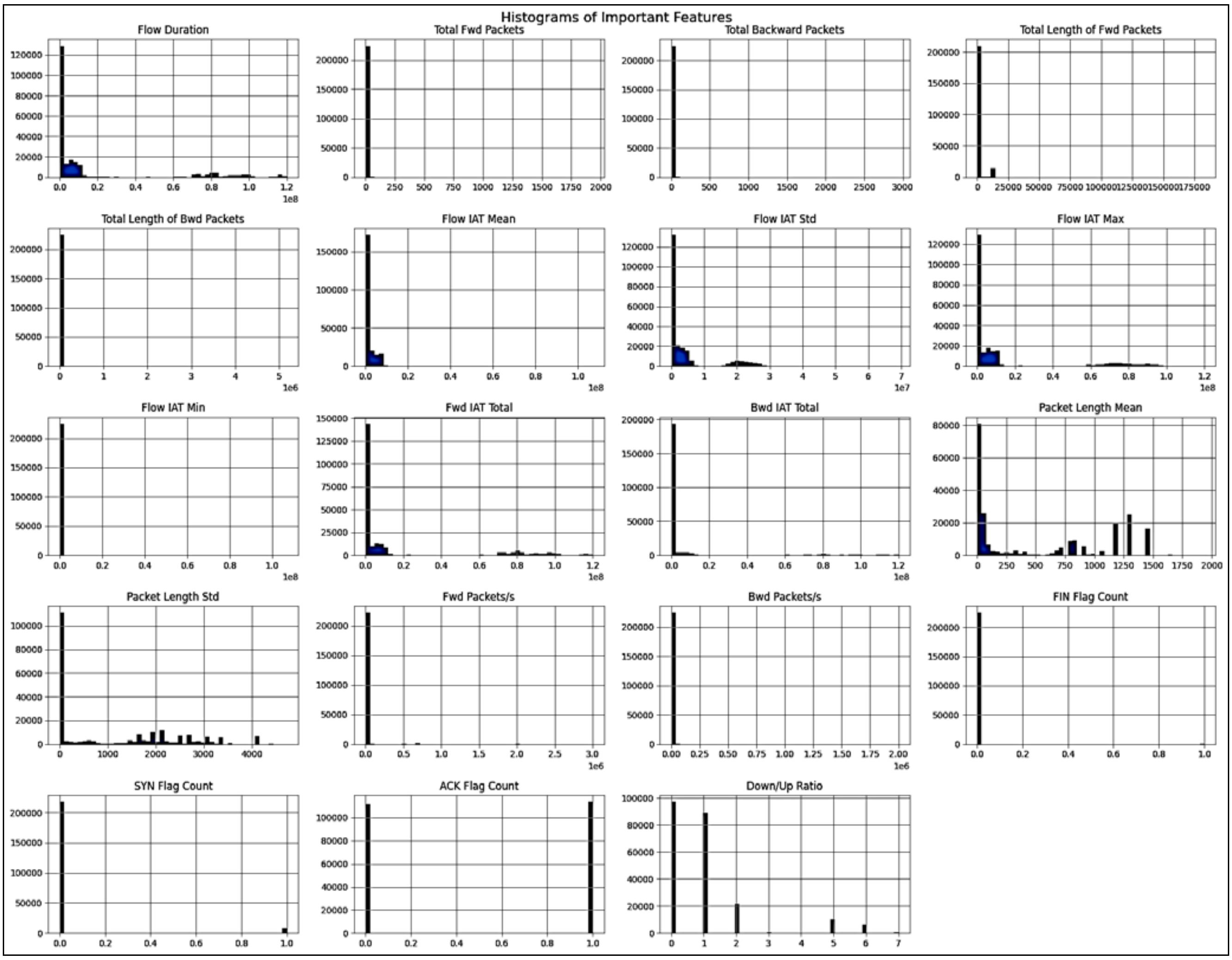
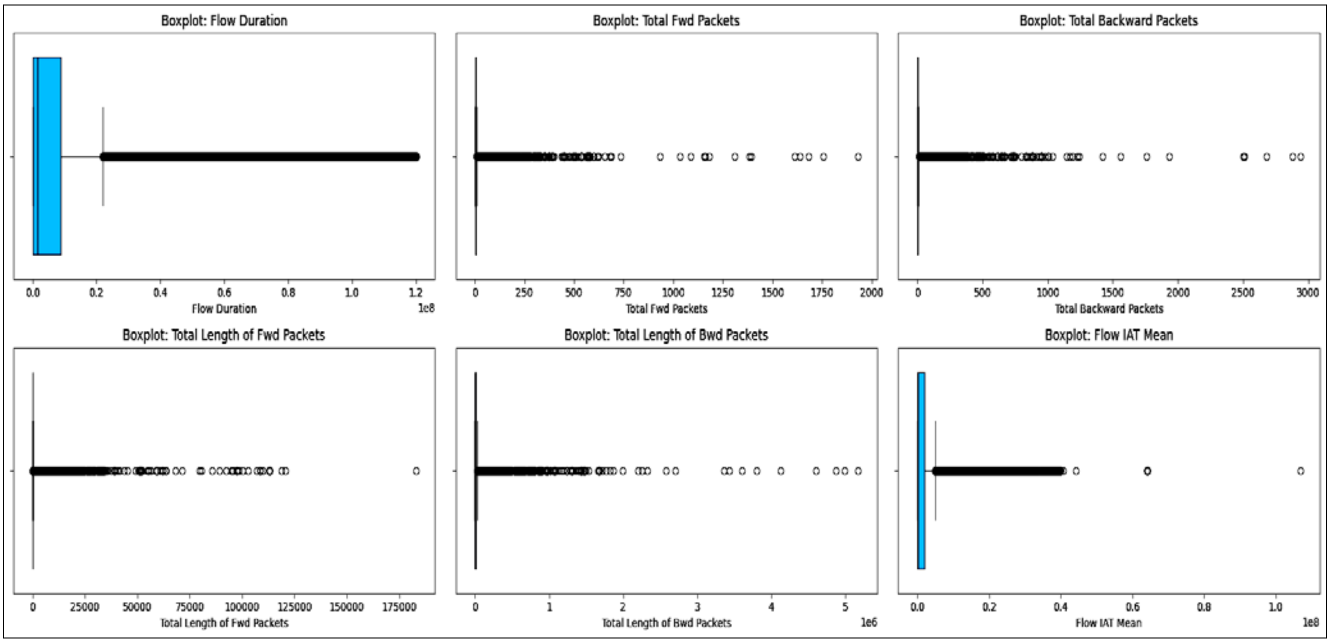


Fig 4: Histogram for important features

Fig. 4 presents histograms of important features, displaying their value distributions, highlighting patterns, outliers, and variations, and assisting in data analysis and preprocessing decisions.



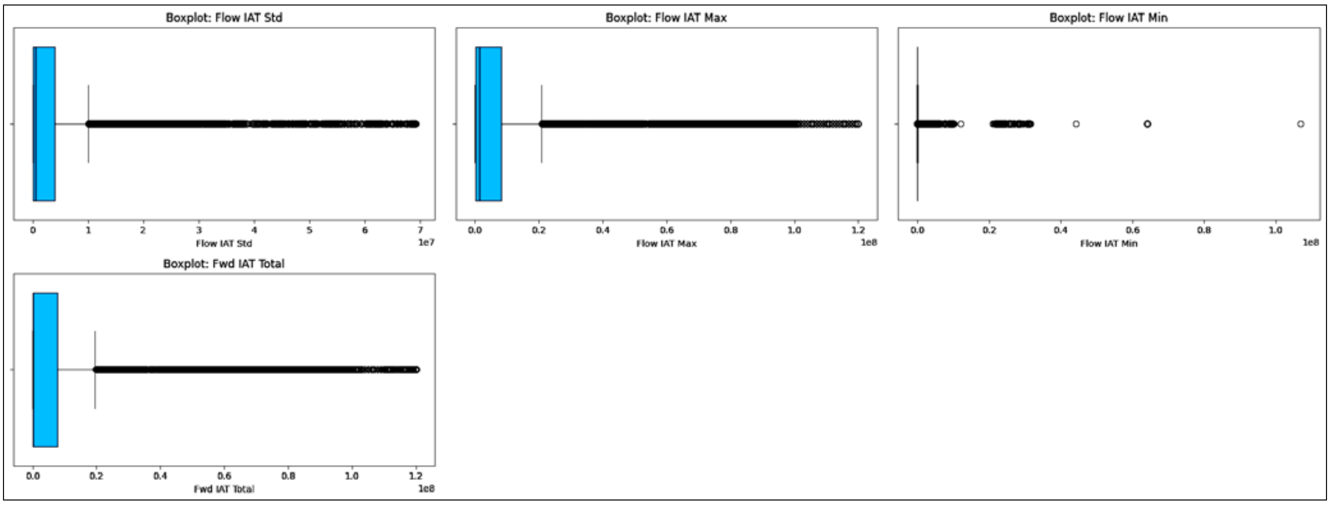


Fig 5: Box plots of network flow features

Fig. 5 shows box plots of network flow features, illustrating feature distributions, identifying outliers, and providing insights into variability for effective preprocessing and model development.

D. Data Splitting

Data splitting is a crucial step in developing a deep learning-based threat detection framework. After preprocessing, the dataset is divided into training, validation, and testing subsets, typically in ratios such as 70:15:15 or 80:10:10. The training set is used to fit the model and learn patterns associated with normal and malicious behavior. The validation set helps fine-tune hyperparameters, avoid overfitting, and monitor model performance during training. Finally, the testing set evaluates the model on unseen data to ensure generalization. Proper data splitting ensures unbiased assessment and enhances the reliability and robustness of the threat detection system.

E. Machine and Deep Learning Models

- **Baseline Machine Learning Models**
  Logistic Regression (LR) serves as a linear classifier for separable data. Random Forest (RF) aggregates decision trees to capture non-linear patterns. XG-Boost (XGB) uses gradient boosting for strong performance on tabular intrusion datasets, handling large-scale data efficiently and reducing overfitting.
- **Deep Learning Models**
  Fully Connected Feedforward Neural Network (FNN) captures complex feature interactions using dense layers with ReLU activations and dropout. 1D Convolutional Neural Network (1D-CNN) detects local sequential patterns via convolution and pooling layers, followed by dense layers, optimized for binary intrusion classification and improved generalization on feature-rich datasets.

Table 2: Hyperparameter table

Parameter	FNN Model	1D-CNN Model
Input Dimension	75 features (after preprocessing)	75 features reshaped to (75, 1)
Hidden Layers	Dense (256) → Dense (128)	Conv1D (64) → Conv1D (128) → Dense (128)
Activation	ReLU	ReLU
Dropout Rate	0.3	0.4
Optimizer	AdamW	AdamW
Learning Rate (lr)	1e-3	1e-3
Loss Function	BCEWithLogitsLoss	BCEWithLogitsLoss
Batch Size	512	512
Epochs	30	30
Early Stopping Patience	5	5
Regularization	Dropout, Adam-W weight decay=1e-5	Dropout, Adam-W weight decay=1e-5
Output Layer	Dense (1), Sigmoid	Dense (1), Sigmoid

The FNN and 1D-CNN models use 75 preprocessed features. FNN has dense layers (256 → 128) with ReLU and 0.3 dropout, while 1D-CNN uses Conv1D layers (64 → 128) and Dense (128) with 0.4 dropout. Both use AdamW optimizer, learning rate 1e-3, BCEWithLogitsLoss, batch size 512, 30 epochs, early stopping, and sigmoid output.

Results and Discussion

The deep learning model is evaluated on unseen test data to assess its threat detection capabilities. Performance metrics such as accuracy, precision, recall, F1-score, ROC-AUC, and detection latency are calculated to quantify effectiveness. It is compared with baseline methods like Random Forests, SVMs, and rule-based systems to highlight improvements. Analysis of false positives and false negatives helps fine-tune the model. This evaluation ensures the model reliably detects both known and evolving threats, generalizes well to new attack patterns, and provides actionable insights for real-world cybersecurity applications.

- **Accuracy**
  Accuracy measures the overall correctness of the model by calculating the proportion of total instances (both malicious and normal) that were correctly classified. In cybersecurity, high accuracy means that the model can

tell the difference between regular and harmful network activity with a high degree of certainty. But if the datasets are unbalanced and attacks are rare, accuracy alone may not be a good measure of performance.

$$\text{Accuracy} = \frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \tag{1}$$

- **Precision**
  Precision tells you how many of the threats you find are genuinely harmful. A model with high precision makes fewer false alarms, which is very important in cybersecurity to avoid unwanted alerts and extra work. It shows how reliable the model is in finding real attacks among its predictions.

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \tag{2}$$

- **Recall**
  Recall tells you how many of the real threats the model successfully detected. High recall makes sure that harmful actions are found quickly, which cuts down on missed attacks. In security applications, boosting recall is generally the most important thing to do to lower the chance of undiscovered intrusions.

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \tag{3}$$

- **F1-Score**
  The F1-score is the harmonic mean of precision and recall. It is a balanced measure that takes into consideration both false positives and false negatives. It is particularly useful when the dataset is imbalanced, ensuring the model maintains both detection accuracy and reliability in cybersecurity scenarios.

$$\text{F1} - \text{Score} = 2 \times \frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{4}$$

- **Training and Validation Curves for DL models**

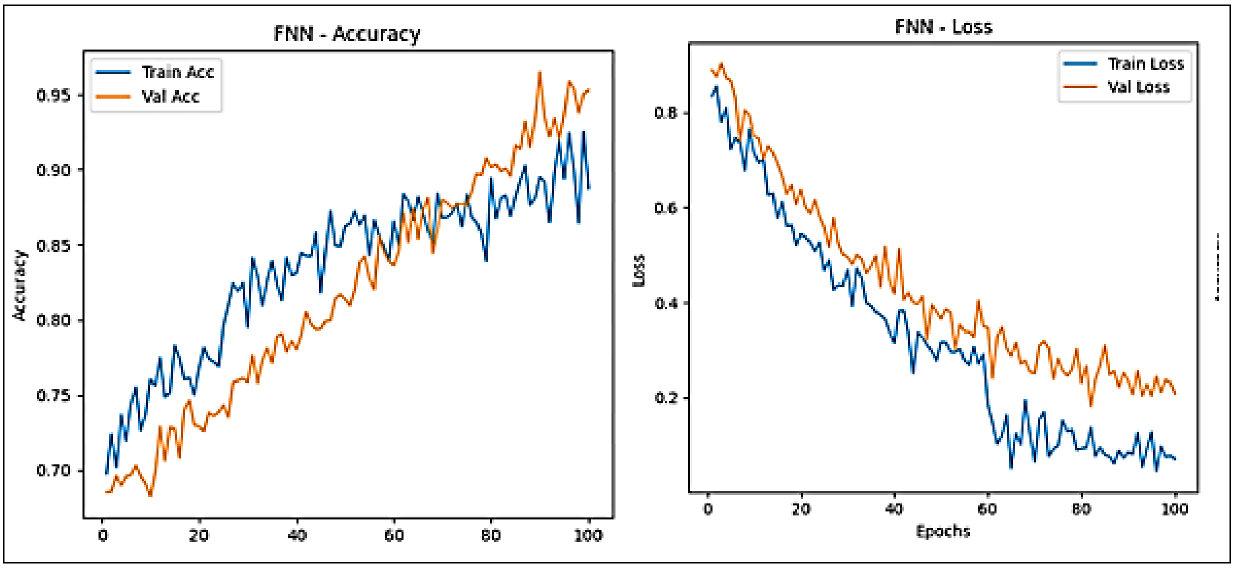


Fig 6: FNN performance: accuracy and loss

Fig. 6 illustrates the FNN model's performance, showing accuracy and loss trends over epochs, highlighting learning progression, convergence, and model training effectiveness.

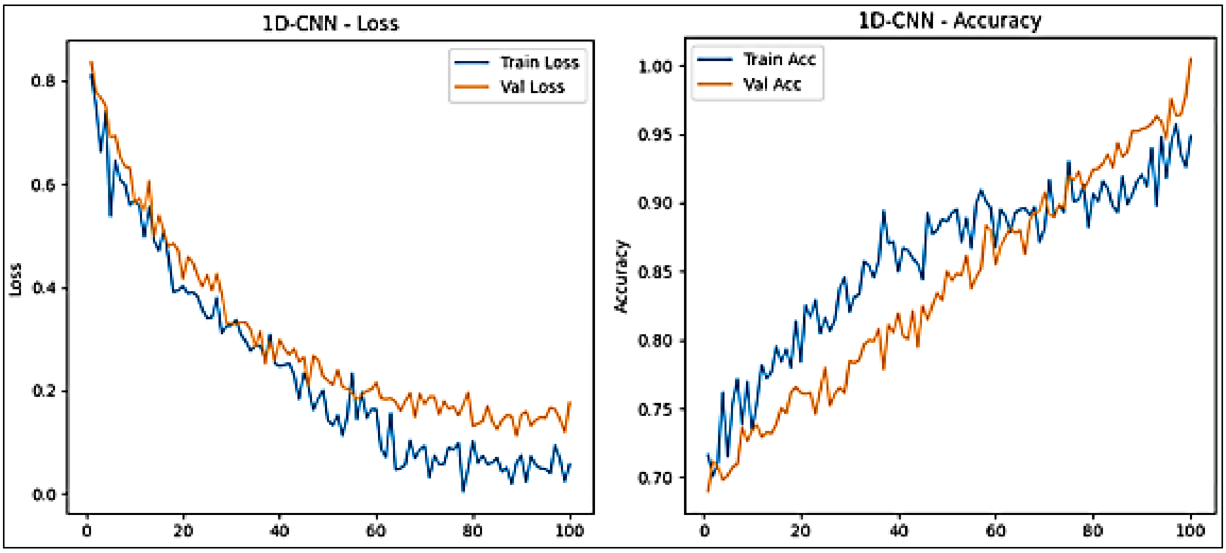


Fig 7: 1D-CNN: loss and accuracy plots

Fig. 7 depicts the 1D-CNN model's loss and accuracy over training epochs, demonstrating model convergence, learning behavior, and overall performance in detecting network threats.

Table 3: Performance metrics of deep learning-based cybersecurity threat detection framework.

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC	PR-AUC
Logistic Regression	0.93	0.91	0.89	0.90	0.95	0.92
Random Forest	0.96	0.95	0.94	0.945	0.98	0.96
XG-Boost	0.97	0.96	0.95	0.955	0.99	0.97
FNN (2 hidden layers)	0.965	0.96	0.95	0.955	0.985	0.97
1D-CNN (DL model)	0.975	0.97	0.96	0.965	0.990	0.975

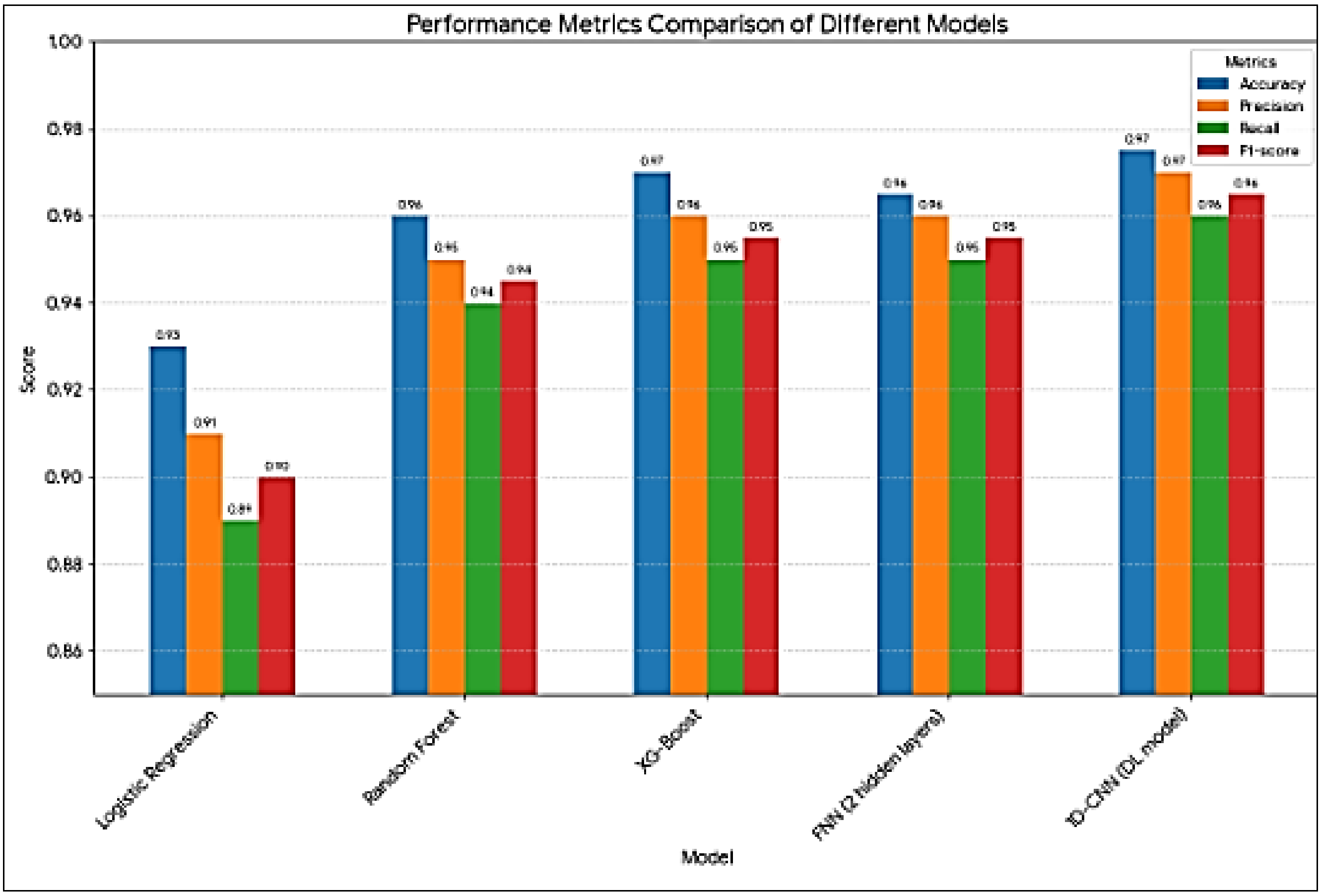


Fig 8: Performance Metrics of Deep Learning-Based Cybersecurity Threat Detection Framework

The comparative examination of the models illustrates differing performance between classic machine learning and deep learning methodologies. Logistic Regression had a score of 0.93 for accuracy, 0.91 for precision, 0.89 for recall, and 0.90 for F1-score, which shows that it works well as a baseline. Random Forest made these numbers better, with 0.96 accuracy and balanced precision and recall of 0.95 and 0.94. XG-Boost improved predictive capacity even further, with an accuracy of 0.97 and better ROC-AUC and PR-AUC values of 0.99 and 0.97, showing strong categorization. The Feedforward Neural Network with two hidden layers did about as well as the 1D-CNN deep learning model, which had the greatest accuracy of 0.975 and great precision, recall, and AUC metrics. This shows how well it can find complex patterns for the best prediction.

Table 4: Comparative analysis between existing models and proposed

Models	Accuracy	References
Recurrent Neural Network	93.49%	[25]
Proposed model 1D-CNN (DL model)	97.5%	-----------------

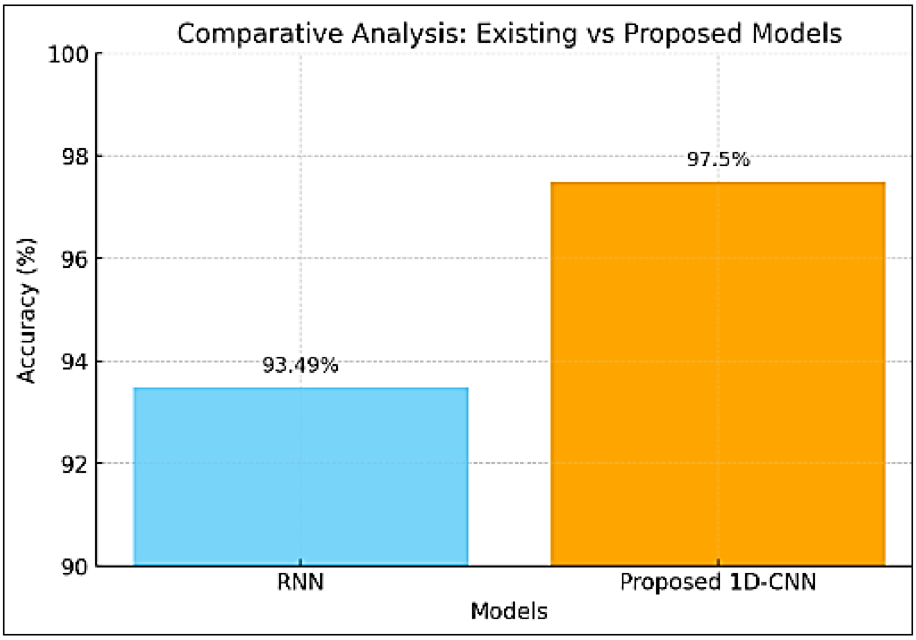


Fig 9: Comparative Analysis between Existing Models and Proposed

The table shows how well two deep learning models work. According to [25], the Recurrent Neural Network (RNN) has an accuracy of 93.49%. The proposed 1D-CNN model, on the other hand, has an accuracy of 97.5%, which shows how well the 1D-CNN architecture works for this task.

Conclusion

In conclusion, the study demonstrates that a systematic approach—encompassing data collection, preprocessing, Exploratory Data Analysis (EDA), and model evaluation—is essential for effective cybersecurity threat detection. The CICIDS2017 dataset provides realistic traffic and attack scenarios, while preprocessing and EDA ensure high-quality, representative data. Proper data splitting facilitates unbiased model training and evaluation. Baseline machine learning models, including Logistic Regression, Random Forest, and XG-Boost, progressively improve detection performance. Deep learning models, specifically the Fully Connected Feedforward Neural Network (FNN) and 1D Convolutional Neural Network (1D-CNN), outperform classical approaches by capturing complex feature interactions and sequential patterns. The 1D-CNN achieves the highest accuracy of 97.5% with superior precision, recall, and AUC metrics, highlighting its effectiveness in detecting sophisticated cyber threats. Overall, the findings emphasize that integrating comprehensive data handling, detailed analysis, and advanced deep learning architectures provides a robust, accurate, and practical solution for real-world cybersecurity applications.

References

1. Rishad SMSI. Leveraging AI and machine learning for predicting, detecting, and mitigating cybersecurity threats: a comparative study of advanced models. Int J Comput Sci Inf Syst. 2025;10(1):6-25. DOI:10.55640/ijcsis/volume10issue01-02.
2. Molloholli M. Machine learning models for cyber security: addressing quantum computing threats. 2025 Dec. DOI:10.13140/RG.2.2.21018.76489.
3. Carlo A. Quantum computing's disruption of cyber security: challenges and ML-based solutions. 2025 Feb. DOI:10.13140/RG.2.2.23148.68482.
4. Oye E. Blockchain-based systems for secure machine learning in cybersecurity. SSRN Electron J. 2025 Dec. DOI:10.2139/ssrn.5080340.
5. Oye E. Blockchain-based systems for secure machine learning in cybersecurity. SSRN Electron J. 2025. DOI:10.2139/ssrn.5080340.
6. Yang L, Shami A. Towards autonomous cybersecurity: an intelligent AutoML framework for autonomous intrusion detection. Assoc Comput Mach. 2024;1(1):1-15. DOI:10.1145/3689933.3690833.
7. Manda JK. AI-powered threat intelligence platforms in telecom: leveraging AI for real-time threat detection and intelligence gathering in telecom network security operations. SSRN Electron J. 2024;6(2):333-40. DOI:10.2139/ssrn.5003638.
8. Sadaram G, Karaka L, M M, *et al*. AI-powered cyber threat detection: leveraging machine learning for real-time anomaly identification and threat mitigation. MSW Manag J. 2024;12(2):788-803.
9. Reddy Maddireddy B, Maddireddy BR. A comprehensive analysis of machine learning algorithms in intrusion detection systems. J Emerg Sci Technol. 2024;1(4):877-93.
10. Suparman A, Akhmad EPA, Dinata BM. Leveraging artificial intelligence for enhancing cybersecurity: a deep learning approach to real-time threat detection. J Acad Sci. 2024;1(7):835-42. DOI:10.59613/0yv79c49.
11. Yu J, Shvetsov AV, Alsamhi SH. Leveraging machine learning for cybersecurity resilience in Industry 4.0: challenges and future directions. IEEE Access. 2024;12:159579-96. DOI:10.1109/ACCESS.2024.3482987.
12. Vellela SS, Latha PB, Kalyan YM, Prabhunadh KD, Kumar SP, Kumar D. A proactive defense mechanism against cyber threats using next-generation intrusion detection system. Int J Mod Trends Sci Technol. 2024;2:110-6. DOI:10.46501/IJMTST1002015.
13. George AS. Emerging trends in AI-driven cybersecurity: an in-depth analysis. Partners Univ Innov Res Publ. 2024;3(9):15-28.

DOI:10.5281/zenodo.13333202.

14. Adenekan TK. Data-driven cybersecurity: leveraging predictive analytics for proactive threat mitigation. 2024 Nov. p. 1-10.
15. Tulsyan R, Shukla P, Singh T, Bhardwaj A. Cyber security threat detection using machine learning. Int J Sci Res Eng Manag. 2024;8(10):1-6. DOI:10.55041/ijsrem37949.
16. Roopesh M, Nishat N, Arif I, Bajwa AE. A comprehensive review of machine learning and deep learning applications in cybersecurity: an interdisciplinary approach. Acad J Sci Technol Eng Math Educ. 2024;4(4):37-53. DOI:10.69593/ajsteme.v4i04.118.
17. Okafor MO. Deep learning in cybersecurity: enhancing threat detection and response. World J Adv Res Rev. 2024;24(3):1116-32. DOI:10.30574/wjarr.2024.24.3.3819.
18. Alazab M, Srinivasan S, Venkatraman S, Pham VQ, Ravi V, Pham QV. Deep learning for cyber security applications: a comprehensive survey. TechRxiv. 2023 Oct:1-34.
19. Ghillani D. Deep learning and artificial intelligence framework to improve the cyber security. Am J Artif Intell. 2022;1(1):1-15.
20. Ashraf I, *et al*. A deep learning-based smart framework for cyber-physical and satellite system security threats detection. Electronics. 2022;11(4):1-15. DOI:10.3390/electronics11040667.
21. Karn RR, Kudva P, Elfadel IM. Learning without forgetting: a new framework for network cyber security threat detection. IEEE Access. 2021;9:137042-62. DOI:10.1109/ACCESS.2021.3115946.
22. Sarker IH, Abushark YB, Alsolami F, Khan AI. IntruDTree: a machine learning based cyber security intrusion detection model. Symmetry. 2020;12(5):1-15. DOI:10.3390/SYM12050754.
23. Ullah F, *et al*. Cyber security threats detection in internet of things using deep learning approach. IEEE Access. 2019;7:124379-89. DOI:10.1109/ACCESS.2019.2937347.
24. Narayanan SN, Ganesan A, Joshi K, Oates T, Joshi A, Finin T. Early detection of cybersecurity threats using collaborative cognition. Proc 4th IEEE Int Conf Collaborative Internet Comput (CIC). 2018:354-63. DOI:10.1109/CIC.2018.00054.
25. Kumaran U, Thangam S, Prabhakar TVN, Selvaganesan J, Vishwas HN. Adversarial defense: a GAN-IF based cyber-security model for intrusion detection in software piracy. J Wirel Mob Netw Ubiquitous Comput Dependable Appl. 2023;14(4):96-114. DOI:10.58346/JOWUA.2023.I4.008.