International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 15 Issue 3, March-2026

AI-Enhanced Cybersecurity System for Detecting and Preventing Network Attacks

Mr. Kiran Devanand Ibitkar[1], Prof. Dr. Monika Rokade[2],
Prof. Dr. Sunil Khatal[3]

[1]Student, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune. India
[2]Project Guide, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune. India
[3]HOD, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune. India

ABSTRACT

The speed of cloud computing, the Internet of Things, and large-scale systems using distributed networks has altered the general landscape of what modern cyberattacks exploit. As a result, the more sophisticated types of cyberattacks pose daunting challenges to the cybersecurity attacks, like the Distributed Denial-of-Service attacks, the reconnaissance, or the malicious software that spreads across a network. What has worked for years, like firewalls and the rule-based Intrusion Detection System, is failing to recognize the new, sophisticated attack vectors emerging almost daily. This situation, specifically the complex and novel types of attacks that the cybersecurity mechanisms have employed, requires the on-the-fly development of intelligent, highly adaptable, and automated security mechanisms to interpret and respond to the complex network behavior in real time. For this research an Artificial Intelligence-based Threat Detection and Prevention System (TDPS) is constructed on the NSL-KDD dataset. Artificial Intelligence is constructed based on a series of organized steps which include data preprocessing, data partitioning, and data standardization. As part of that organized series, data partitioning is done in two classes, i.e. for it to go through one of two organized, i.e. data standardization, one of two classification techniques (Random forrest (RF) or Recurrent Neural Network (RNN)), and one of two organized, therefore data partitioning, i.e. data preprocessing, also performed in one of two organized classification systems. Also, one of two organized, i.e. data partitioning, is performed standardization. From the experiments, the Random Forrest model achieved an accuracy of 92.14% and the Recurrent Neural Network model accomplished an accuracy of 96.98% and superior F1 Score Precision and Recall. We can consider that finding is showing us the state of the art deep learning describes better and more sophisticated network behavioral because of the prevalence of sequences of behavior we are left with some significant positioning within the state of the art deep learning. Overall, this system shows how Artificial Intelligence can improve cybersecurity frameworks. It shows how detection accuracy can be improved, false alarms reduced, and it increases protection from new types of threats. The research futhers supports the idea that hybrid AI-based intrusion detection systems provide a good and possibly effective approach to creating the cybersecurity protection systems of the future.

Keywords— ***Cybersecurity, Intrusion Detection System, Machine Learning, Deep Learning, Random Forest, Recurrent Neural Network.***

I. INTRODUCTION

Advancements in digital technology, especially cloud computing, the Internet of Things (IoT), and large-scale distributed systems, have revolutionized the modern world and network infrastructures. They have also led to several critical challenges in cybersecurity, where attackers develop sophisticated techniques to maximize the exploitation of system weaknesses With rapid dynamic and large-scale environments, traditional security systems, such as firewalls and signature-based intrusion detection systems, become inefficient in detection and prevention. Consequently, systems demand foresight in adaptive and intelligent real-time cybersecurity solutions that can proactively address the issues and challenges of modern infrastructures.

The use of Artificial Intelligence (AI), especially Machine Learning (ML) and Deep Learning (DL), in cybersecurity has

proven to be one of the fastest ways to advance security systems. ML-based intrusion detection systems can process massive volumes of network traffic data more efficiently, in comparison to rule-based systems, and successfully identify anomalous behavior and potential threats. On top of that, due to the imbalanced data, the trade-off between detection performance and false alarm rate can become less severe, and detection of anomalies can be improved through an ML based approach [1][2]. A greater advantage of the AI-driven models includes the capability of learning from historical data, and adapting to largely unknown and unseen attack patterns, thus, they can be readily implemented to tackle modern challenges [3][4].

The ability of a system to classify raw input is surprising to many. RNNs are powerful tools because of a climbing demand to classify complex data. These models are distinct because of their application in networks to discover time-based attack behavior. Deep models utilize neural networks to a higher degree explain intrusion detection systems. RNNs are the tool of choice given their abilities to classify sequential data. Also, modestly hybrid models employ a combination of AI systems to work in detection data and offer a higher value per work complex worth data and other realms. These systems provide adequate defense of an organization. In the ICS field and other systems such as national and other related smart grids, responsible systems work to implement intelligent solutions, and these systems have ensured the safe operation of a system. Substantial unwanted events of an operations system. In workplaces of another field intrusion Industry 4.0 manufacturing systems, smart systems that employ Mixed really Constructed and Lowest degree networks attempt to best work to protect the systems. These smart systems have even still greater detection and even greater systems.

These systems still have a high index of unwanted issues, data, and a logical complex system persist. With these and other concerns there is still a need to work to provide a system detection and provide the system with work- and to a protection system of precision limits. This research introduces an AI-based Threat Detection and Prevention System (TDPS), focusing on the combination of both forms of Learning to boost the system's detection capabilities. The proposed system uses the NSL-KDD dataset and employs methods such as preparation, feature extraction, normalization, and classification. Two of the methods, Random Forest and Recurrent Neural Network, are used to distinguish between harmful activities and normal activities. The results of the experiments show that the system significantly improves detection accuracy and decreases the number of false positives, thus helping in the building of more advanced cybersecurity systems

II LITERATURE REVIEW

Alzaylaee et al. [1] designed a next-gen cybersecurity defense system using artificial intelligence with computer vision and machine learning that enables detection of cyber threats as they are occurring. They explain that through the combination of visual data analysis and the aid of AI, the identification of cyber threats into a rapidly changing world can improve. Conventional methods are improved with this study, showing that detection accuracy is higher and the time taken to respond is shorter. This study highlights that, in the design of cybersecurity systems, the integration of real time detection and response systems is key

Sinha et al. [2] designed a machine learning based framework to detect and defend cyber-attacks against industrial cyber-physical systems. The authors chose a focus on the protection of critical infrastructure through the behavior analysis of systems and the detection of anomalies. Their approach enhances the practicality of the system and ease of stability. The authors' findings suggest that the use of machine learning techniques can empower industrial systems against cyber threats.

Ang et al. [3] proposed a multi-layered and adaptive cybersecurity framework for the banking industry. The model integrates next-gen firewalls with AI-based intrusion detection and intrusion prevention systems (IDPS). Their study proves that layered security system integration defense against complex and emerging threats is effective. The framework also proves to improve the adaptability and response time in financial realms.

Rasheed et al. [4] described how data networking and cybersecurity are changing because of artificial intelligence. In this research it is explained how AI can automate the recognition of threats and also an improvement in controlling the network. They show the weaknesses of the traditional methods and suggest the use of intelligent systems for an offensive defense. They have determined that these solutions make the handling of modern cyber threats possible.

Kabir et al. [5] introduced an AI-integrated cybersecurity solution based on the Zero Trust principle for defense of important infrastructure systems. The proposed solution combines modernized secure networks with AI-integrated threats. Their approach claimed a continuous verification on Users and Devices, limiting the chances of unfriendly use. Their tests showed a positive outcome regarding system safety in important critical networks.

Arora [6] discussed the changes that are happening to Cybersecurity Threat Detection Systems (CTDS) via the use of artificial intelligence. The changes included the ability to identify and to address sophisticated threats consistently. Other integrated systems (both civilian and military) would see the added value of conducting AI to help improve operator support

and reduce the existing defense burden. These systems would observe improved safety, speed, and responsiveness.
Sathyabama and Jeevaa Katiravan [7] described a blockchain and deep learning cybersecurity approach taking place in IoT environments. Their model presented an enhancement in anomaly detection as well as the ability to secure data integrity and security in a decentralized manner. The promising results indicate a substantial improvement in Trust and Transparency in IoT systems. Findings indicate a sizable advantage in cybersecurity threat detection and prevention.

Kandasamy and Ameelia Roseline [8] developed a hybrid deep learning model for MITM attack detection in real time. Their model implemented neural networks to determine even the slightest anomalous communications. Their model achieved a high rate of success with an even lower rate of false positives. This study demonstrated the efficacy of deep learning as a method of protection for communication networks.

Rai et al. [9] innovative an AI-prompted IDS that added a great deal of barrier systems to the evolving world of cybersecurity to their advantage. Their model implemented neural networks to analyze an extensive array of data in real time for the purpose of identifying potential threats. Their study displayed enhanced detection capability and adaptability as well as bettered acknowledgment to the established fact of a sizable limitation X to the uncountable systems of IDSs implemented to the essence of the study.

Malik et al. [10] proposed an advanced threat detection and prevention model built to better the changing systems of an already established cybersecurity network. The study upheld their results that revealed improved systems as well as reduced false alarm rates applied to the established fact. Their study came to an even stronger conclusion that virtual systems of a bettered ability of AI systems of even a greater limitation X to the numerous uncountable systems of cybersecurity defense and proof may be further able to be migrated to their reliance.

III. METHODOLOGY

This system is an AI-Enhanced Threat Detection and Prevention System that is intended to detect malicious network activity that can be differentiated from normal network activity. To enhance the accuracy of intrusion detection on the network, the system combines the traditional Machine Learning (Random Forest) with Deep Learning (Recurrent Neural Network) techniques. The methodology is executed on the pipeline of a system that is comprised of various processes including data collection, data preparation, feature selection, model training, model evaluation, and prediction. The optimal model is aimed at providing a defense improvement mechanism for robust cybersecurity such that automatic detection can be conducted for network traffic data DoS, probing and unauthorized access attacks. The system was tailored such that it could perform on benchmark datasets including the NSL-KDD that is widely utilized for assessing intrusion detection systems..

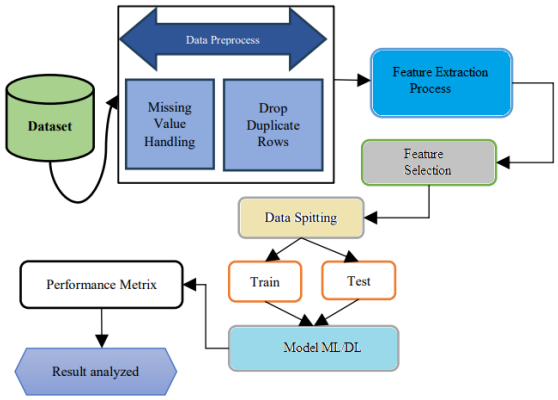

Fig.1 System Architecture

3.1 Dataset Collection

The proposed intrusion detection system uses the KDD/NSL-KDD dataset, as it has become the standard dataset for building and assessing network security models. This dataset contains massive amounts of network connection logs, each described by 41 different, variously characterized network connections.

- These features can be divided into the following, several different types:
- Basic features such as the type of protocol, type of service, and type of connection
- Content features of the connection that describe connections to the payload
- Statistical features of the flow, the behaviors of the network communication.
- Host features relate to the previous connections made from the source or to the destination

Each log entry in the dataset is characterized as normal traffic or as an anomaly (an attack). This characteristic, therefore, is more suited for supervised-learning-based intrusion detection.

.

3.2 Data Preprocessing

The step of data preprocessing is a critical step, indeed, in transforming the raw network traffic data into the format that aligns with the requirements of each of the machine and deep-learning models. Real-world datasets are usually filled with various contradictory cases, missing or empty cases, or duplicated cases, or even cases that are categorized into disjoint sets, that cannot be used in several straight algorithms in an order. In this system, data preprocessing starts with the dataset being loaded into the environment for processing. Where missing cases are encountered, methods for the missing cases are being employed without creating any bias, or influencing the robustness of the model. The cases of duplication are removed in order to reduce the redundancy and to increase the processing performance. Certain features in a dataset are categorical, meaning that must be converted to numerical types. One way to do that is to use one-hot encoding, which assigns binary numbers to categorical types. Some features, in this data set, are protocol types, services, and flags which are used to define types of communication in a network. After this steps, a dataset is prepared for any machine learning or deep learning techniques to be applied.

3.3 Feature Extraction

During the feature extraction phase, essential numerical and normal features are derived from the raw text data. Various techniques—such as correlation-based methods, co-occurrence analysis, relational feature extraction, and dependency-based features—are applied to obtain meaningful representations while eliminating irrelevant attributes from the dataset.

3.4 Feature Selection

Identifying hidden patterns in traffic is one of the most important aspects for any network. Features which makes a user's model better is the incorporation of additional statistical network derived features that explain the inner workings of the network traffic. These features explain the distributions and flows of network, and the behavior of the network. They ultimately enhance traffic and network anomaly detection, thus better intrusion detection.
The following features come from the processed dataset:

- Sum: The total magnitude of network features.
- Mean: The average network traffic features.
- Max: The maximum feature value within the set.
- Min: The minimum feature value within the set.
- Standard Deviation: The dispersion of features from their average value.
- Energy: The magnitude of the features.
- Zero: The number of features set at 0.

The new features result in better learning of the models due to richer features of network behavior. They have also significantly improved anomaly detection and normal traffic distinction from malicious traffic.

3.5 Data Splitting

After feature extraction and preprocessing, the dataset is split into training and a test set. This allows assessing the model's performance in handling data outside the training set.
The dataset is split in the following ratio:

- Training Set: 80%
- Testing Set: 20%

The training set is used for model creation and optimization. The testing set is used for evaluating model performance. This creates a framework for an unbiased assessment of the model and allows for an accurate estimation of the model's ability to generalize.

Machine Learning and Deep Learning Classifier: Random Forest

Random Forest is a classification algorithm, part of ensemble learning, that is widely used for solving many classification problems, including intrusion detection. This algorithm constructs multiple decision trees during the training phase and combines their output for the final prediction. Decision trees of a Random Forest model predict labels in a binary classification of attack or normal and subsequently vote using a majority rule in class determination for the purpose of better accuracy in predictions. Random subsets of the feature set and the data set in model training diversifies the model and

decrease the likelihood of overfitting.
Random Forest models show improved predictive capabilities for high dimension data and are useful and provide robust predictive baselines for network data and anomaly detection.

RNN and LSTM
The models in this chapter use recurrent networks as a form of artificial networks in deep learning. As the name suggests, recurrent networks utilize models that capture sequential data. LSTM are a special class of recurrent network. RNN are useful for detecting data sequential patterns and are used here for that purpose.

For most unsupervised or sequential data, the units of RNN use in this work would be considered to be LSTM networks because of their ability to learn long-range patterns. Given this fact, the units for the RNN used in this work are LSTM units. Here, the RNN comprised of the following:

- Input layer
- Dropout Layer with a rate of = 0.3
- LSTM layer of 64 neurons
- Softmax Output layer

The model is provided a certain number of estimations over the course of 150 epochs using the Adam optimizer and a learning rate of 0.3.

The Dropout layer would perform a form of stochastic learning on network classes whereas the LSTM would learn the data over a time parameter.

Performance Evaluation Metrics
The performance of the proposed system is assessed using common classification metrics sourced from the confusion matrix, which includes how well the model identifies malicious traffic from the normal traffic.

The main evaluation metrics include:

- Accuracy
- Precision
- Recall
- F1-score

All these parameters provide an all-round evaluation of the level of the model performance, particularly on the unbalanced cybersecurity datasets

Algorithm
1: Data Preprocessing and Feature Extraction and selection
Input: NSL-KDD Dataset
Output: Processed Dataset
Step 1: Upload dataset File
  Step 2: Handle missing values
  If missing values exist, then
    Replace with mean/mode or remove records
  End If
  Step 3: Remove duplicate records
  Remove duplicate entries
  Step 4: Encode categorical features
  For each categorical attribute (protocol_type, service, flag) do
    Apply One-Hot Encoding
  End For
Step 5: Normalize numerical features
  For each numerical feature do
    Apply Min-Max Scaling
  End For
Step 6: Feature extraction
  For each record do

Compute Sum
Compute Mean
Compute Maximum
Compute Minimum
Compute Standard Deviation
Compute Energy
Compute Zero Count
End For
Return processed dataset
End

Algorithm 2: Random Forest Training

Input: Training Dataset
Output: Trained Random Forest Model
Step 1: Load training dataset
Step 2: Initialize Random Forest with N trees
For each tree in forest do
Select random subset of data (bootstrap sampling)
Select random subset of features
Build decision tree using selected data
End For
Step 3: Combine all trees to form Random Forest model
Return trained model
End

Algorithm 3: RNN (LSTM) Training

Input: Training Dataset
Output: Trained RNN Model
Step 1: Load training dataset
Step 2: Convert dataset into 3D tensor format
(Samples × TimeSteps × Features)
Step 3: Initialize model architecture:
Input Layer
LSTM Layer (64 neurons)
Dropout Layer (rate = 0.3)
Softmax Output Layer
Set optimizer = Adam
Set activation function = Tanh
Set number of epochs = 150
For epoch = 1 to 150 do
Feed training data into network
Perform forward propagation
Compute loss (cross-entropy)
Perform backpropagation
Update weights
End For
Save trained RNN model
Return trained model
End

Algorithm 4: Testing Detection (Prediction Phase)

Input: New Network Traffic Data, Trained Models
Output: Classification Result (Normal / Attack)
Step1: Input new network traffic data
Step2: Apply preprocessing:
Handle missing values
Encode categorical features
Normalize data
Extract statistical features
Step 3: Prediction using models
RF_Prediction ← Random Forest Model(data)

```
   RNN_Prediction ← RNN Model(data)
Step 4:Final decision (optional ensemble)
   If RNN_Prediction == Attack OR RF_Prediction == Attack then
      Output = "Attack Detected"
   Else
      Output = "Normal"
   End If
   Return Output
End
```

IV. RESULTS

Dataset Description

The suggested intrusion detection system gets its performance check from open resources in the networking intrusion datasets. These datasets involve genuine networking records, along with malicious traffic, and records of simulated networking. This is useful in cybersecurity to test out systems performing detection of intrusion at the level of deep and machine learning. The datasets contain a networking connection case, and each case is demonstrated by a given network behavior. Usually, these examples are composed of a network's connections and their structural and content related and even temporal patterns when communicating. This means there are various available network traffic types, and in the datasets, there are a variety of both categorical and numerical data. This variety is the major contributor to the analysis, particularly statistical and analytical machine learning. The datasets consist of 41 features and just one label. The label would specify if the case is an exampere of norm or attack. For most intrusion detection system applications, this adheres to a supervised learning algorithm, making the datasets a major resource.

Table 1: Performance Comparison of Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Random Forest (RF)	92.14	92.42	91.28	92.65
Recurrent Neural Network (RNN)	96.98	97.49	96.00	96.74

Table 1 shows how each model performs when identifying

Network intrusions. The Random Forest model was able to achieve an accuracy of 92.14%. That shows that it was able to classify almost all the network traffic correctly, while attaining a precision score of 92.42%. This shows that it was able to recognize attack incidents while being rather liberal in giving a low false positive rate. The Random Forest model did, in fact, miss a few instances when attacks occurred, and that was reflected in the recall value of 91.28%. This model was able to achieve a result of 92.65% of the F1 score, showing that it was able to find a good balance between recall and precision. Compared to this, the Recurrent Neural Network (RNN) model was able to outperform the Random Forest model in all the evaluated metrics, demonstrating the RNN was able to classify better, and achieve an accuracy of 96.98%. This was also due to the model's elite ability to identify malicious traffic, while having an average precision of 97.49% for fine-tuning false alarms. The recall of the RNN was able to achieve a 96% for strongly identifying attack incidents, and the F1 score of 96.74% showed the RNN model's fine-tuning of precision and recall was elite.

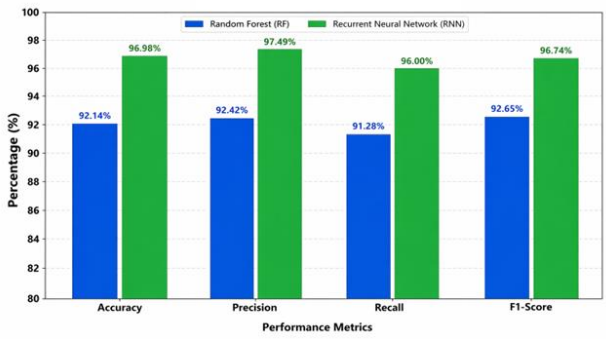

Figure 2: Model Performance Comparison

Figure 2 compares the Random Forest (RF) and Recurrent Neural Network (RNN) models across the four key performance metrics: Accuracy, Precision, Recall, and F1-Score. The results show that on all the key performance metrics, Random Forest is consistently less effective when compared to RMN Models. RNN model has an accuracy of 96.98% while Random Forest has an accuracy of 92.14%. This shows that the RNN Neural Network is more effective when it comes to correctly classifying normal and abnormal network traffic. The Random Forest model is less effective when compared to RNN models on all of the Precision, Recall, and F1 score metrics too. RNN has precision of 97.49%, Random Forest has a precision of 92.42%. When looking at recall, on average across all of the Random Forest models the recall was 91.28%; RNN has a 96% recall. RNN has a 4.74% advantage over Random Forest when it comes to the F1 score, RNN has a 96.74% while Random Forest has a 92.65%. Overall, RNN models are more effective across all models and metrics when compared to Random Forest models. The RNN models are more effective at correctly classifying normal and abnormal network traffic. Random Forest models are less effective across all metrics when compared with RNN models.

CONCLUSION

This study presented an Artificial Intelligence (AI)-based Threat Detection and Prevention System (TDPS) for identifying cyber-attacks in network traffic using the NSL-KDD dataset. The proposed system combines machine learning and deep learning, specifically Random Forest (RF) and Recurrent Neural Network (RNN), for improving the performance of intrusion detection. Preliminary steps of implementation included data preprocessing, followed by feature extraction, normalization, and subsequently model training. These steps were to ensure the dataset was prepared for classification with accuracy. The insertion of statistical feature extraction added further enhancement in representation of network and improved the detection of anomalies. The results of the experiments exhibited that both models performed successfully in the detection of cyber threats. The Random Forest model presented strong baseline performance with an accuracy of 92.14% and was proven to be an effective traditional machine learning model as compared to others, because it was built using the RF algorithm. Yet in the detection of complex and evolving attack patterns, the Random Forest model was shown to be less effective compared with the Recurrent Neural Network model which achieved an accuracy of 96.98% with noted superiority in capturing the normal and attack anomalies as shown in the improved results for precision, recall, F-score, and average performance. Overall results confirm that if deep learning models which follow RNN models are used, there are clear advantages over traditional models. Deep learning techniques improve intrusion detection systems (IDS) both in false positive reduction and detection reliability. Combining artificial intelligence techniques and cybersecurity offer a better defense for crossing the defensive perimeter and a more powerful and adaptable defense for protective boundaries of physical residences/circles in a modern world of Networks. The developed system provides front-lines defense for enterprises and wards off growing threats beyond the defensive perimeter.

REFERENCES

[1] Alzaylaee, Mohammed K., et al. "Advancing Cybersecurity: AI-Driven Computer Vision and Machine Learning Models for Real-Time Threat Detection and Prevention." Journal of Engineering Research (2026).

[2] Sinha, Anurag, et al. "A Machine Learning Framework for Detecting and Preventing Cyber-Attacks in Industrial Cyber-Physical Systems." Engineering Reports 8.1 (2026): e70520.

[3] Ang, Sokroeurn, et al. "A Multi-Layered Adaptive Cybersecurity Framework for the Banking Sector Integrating Next-Gen Firewalls with AI-Driven IDPS." STAP Journal of Security Risk Management 2026.1 (2026): 67-76.

[4] Rasheed, Muhammad Danish, et al. "LEVERAGING ARTIFICIAL INTELLIGENCE FOR ADVANCE DATA NETWORKING AND CYBERSECURITY." Spectrum of Engineering Sciences 4.3 (2026): 286-298.

[5] Kabir, Md Humayun, et al. "Zero Trust Based Critical Infrastructure Cybersecurity Framework with AI-Driven Threat Detection and Secure Network Modernization." Journal of Computer Science and Technology Studies 8.5 (2026): 01-14.

[6] Arora, Anuj. "Transforming cybersecurity threat detection and prevention systems using artificial intelligence." Available at SSRN 5268166 (2025).

[7] AR, Sathyabama, and Jeevaa Katiravan. "Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security." Scientific Reports 15.1 (2025): 22369.

[8] Kandasamy, V., and A. Ameelia Roseline. "Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks." Scientific Reports 15.1 (2025): 1697.

[9] Rai, Hari Mohan, et al. "Advanced AI-powered intrusion detection systems in cybersecurity protocols for network protection." Procedia Computer Science 259 (2025): 140-149.

[10] Malik, Anum, et al. "Artificial intelligence-driven cybersecurity framework using machine learning for advanced threat detection and prevention." Sch. J. Eng. Tech 6 (2025): 401-423