iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** VI **Month of publication:** June 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.83342

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue VI June 2026- Available at www.ijraset.com*

# AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System

Preeti Kumari[1], Roushni Raj[2], Himanshi Bhandari[3], Khushi Goenka[4], Rahul Anjana[5]
*IILM University, India*

***Abstract:*** ***The high-paced growth of Internet of Things (IoT), digital infrastructure, and cloud computing technologies has considerably enhanced the level and rate of cyber-attacks. Traditional security technologies (e.g., signature-based Intrusion Detection Systems (IDS) and firewalls) are not adequate to identify zero-day exploits, polymorphic malware, and advanced persistent threats because they are based on known attack patterns. In order to overcome these constraints, this paper presents a proposal of the AI-Based Cyber Attack Detection and Prevention System that applies to the intelligent detection of threats and automated prevention through the application of the techniques of Machine Learning (ML) and Deep Learning (DL). The suggested framework incorporates supervised learning such as the random forest and Support Vector Machine (SVM) and Artificial Neural Networks (ANN) in detecting anomalies and classifying traffic. The system examines network flow characteristics and behaviour patterns in order to detect maliciousness like DDoS, phishing, malware injection, and attempted unauthorized access. There is an automated prevention module which prevents suspicious IP addresses and isolates compromised nodes on the fly. The benchmark evaluation of experimental evaluation based on the cybersecurity datasets shows high accuracy of detection, low rate of false positives and reduced response time as compared to the conventional rule-based systems. The findings confirm the usefulness of artificial intelligence to construct dynamic, scalable and proactive cybersecurity protection systems that can be used by contemporary network systems.***

***Keywords: Artificial intelligence, Cybersecurity, Intrusion detection system, Machine learning, Deep learning, Network security, Threat detection, Threat prevention.***

## I. INTRODUCTION

The astronomical increase in digital transformation in industries has resulted in the high reliance on interconnected systems and online services. Although these developments have enhanced the efficiency of operation and communication globally, they have also made more attack points to cyber adversaries. The emerging cyber threats of today, such as ransomware, Distributed Denial of Service (DDoS) attacks, phishing, insider threats, and Advanced Persistent Threats (APTs) are increasingly dynamic and advanced. Traditional security systems like firewalls, signature-based Intrusion Detection Systems (IDS) are based on pre-defined attack signatures and rule-based systems. Even though they are effective in known threats, they cannot be used to identify novel attacks or zero-day attacks. In addition, the sheer quantity and speed of network traffic present-day settings render manual monitoring and manually configuring rules impractical. As a result, smart security measures that would keep up with the changing patterns of attacks are highly needed. Artificial Intelligence (AI), specifically, Machine Learning (ML) and Deep Learning (DL), is a promising method of fortifying the cybersecurity structures. The AI-based systems have the ability to process extensive data on a network, discover meaningful patterns and spot abnormal behaviours that indicate a possible cyber-attack. In contrast to conventional systems, AI models keep on improving whenever new data is fed to them, through learning, which makes them proactive in detecting threats. The paper stipulates a project idea of an AI-Based Cyber Attack Detection and Prevention System that would increase the level of network security based on the intelligent analysis and automated reaction systems. The system uses feature extraction algorithms to preprocess network traffic data and uses classification algorithms that can differentiate the benign and malicious activities. Also, an integrated prevention module will prevent suspicious traffic automatically, create alerts, and reduce the effects of identified threats. The key contributions of the study are as follows: Design of an AI-based intrusion detection system based on a hybrid ML/DL system. Implementation of real time automated preventive measures. Assessment of the performance based on benchmark cyberspace security data. Comparison with evidence of a better detection and lower false positives. This paper is structured as follows: Section II conducts a literature review; Section III outlines the proposed system architecture; Section IV elaborates the methodology; Section V provides the experimental outcomes and performance analysis; and finally, Section VI of the paper is a conclusion of the paper with regard to future research directions.

©IJRASET: All Rights are Reserved 

Artificial intelligence is the capability to think, comprehend, discern patterns, remember, make decisions out of the numerous alternatives, and to learn through experience. The goal of artificial intelligence is to provide a computer that is capable of faking the functions of the human brain so that computers can follow through with all the functions that humans carry out within a fraction of the time. Current AI breakthroughs have affected politics, media, games, and even public life. Politics Artificial Intelligence was applied to achieve better utilization of resources, energy, and time in the election campaign to reach the target audience. The current governments, organizations, and institutions are susceptible to cyber-attacks. Approximately 200 million personal records were disclosed due to data breaches at the Federal Bureau of Investigation (FBI) and the Department of Homeland Security, and some of the most high-profile data releases. As of now, it is just a gradual and a restricted effort to work out what the other individuals are trying to accomplish. In the opinion of the Forbes, the computer security market in the entire world is likely to reach 170 billion by 2020. The increased development of technology and a whirl of activities that keep security standards on the move are the most significant factors that prominently contribute to the fast growth of the market. The issue of cyber security is a burning topic nowadays, and it is being implemented along with Artificial Intelligence. Artificial intelligence based cyber security technologies are proven to be more effective at protecting and securing digital data.

The Artificial Intelligence (AI) can be of great help in fighting such threats. Artificial Intelligence has the potential to be a useful partner when it comes to building a line of defence against hackers. Artificial Intelligence can be trained to be able to continually identify trends and learn them so that any deviations will be identified. Machine learning is significant in Artificial Intelligence. It continuously enhances its operations and finds preventative methods of fighting off threats in the future through the information that it gathers. Its capability to study and comprehend human behaviour, as well as, identify trends and see even minor discontinuities to those trends, renders it Cybersecurity-suited. This data can also be exploited by Artificial Intelligence to build its plans and operations. The greatest ambition of Artificial Intelligence is to create technology that would enable the computer systems to operate in a smart manner. Regarding cybersecurity, AI could be applied to detect new vulnerabilities faster and with high accuracy to prevent the occurrence of attacks in the future.

In addition to traditional machine learning models this work introduces a hybrid approach by combining supervised learning with semi-supervised anomaly detection.

This enables the system to detect both known and unknown cyber-attacks effectively. A simulated prevention mechanism is incorporated to demonstrate how detected threats can be handled in real-time environments.

### *A. Advantage Of Artificial Intelligence In Cyber Security*

Organizations have to face millions of risks each and every day, which means that defining and analysing this issue is hardly achievable by a cybersecurity company. Machine Learning can be employed to perform this task quickly and effectively.[7]

Organizations will be able to fully leverage the current knowledge of threats and vectors and discover a way to use supervised and unsupervised machine learning.[3] Combining these techniques with a capability to detect the new attacks and locate the new weakness that can destroy the contents will allow the system to protect the content in a much more efficient manner.[8]

1) Error Reduction: In majority of the cases scientists deploy artificial intelligence (AI) with the hope of reducing the danger. Additionally, it raises the likelihood of achieving accuracy with a higher degree of precision.[9]
2) Daily Applications: Automated approach to learning has become widespread in every day's life. Artificial intelligence is commonly used in organizations like Banks to detect fraud users.[9]
3) No Breaks: Machines do not need breaks frequently for refreshments like humans. As machines are programmed for long hours. Also, they can perform for large period of time without getting bored and provide accurate results in minimum time than humans.[9]
4) Increased Work Efficiency: AI-powered devices are extremely efficient in doing repetitive task. The best part is that they remove mistake made by humans from their task to get accurate and precise outcomes.[9]
5) Minimum cost of training and operation: Machine learning methods such as Supervised learning and Artificial neural network are used to learn new information in the same way done by humans. Additionally, it also avoids the requirement to develop new code every time.[9]

### *B. AI as the Future Of Cyber Security*

Nowadays cyber-attack is one of the most serious challenges faced by today's organizations, governments, and institutions.[1] In 2016 data breaches exposed over 200 million personal details, including high-profile thefts at the Department of Homeland Security and the FBI.[20]

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue VI June 2026- Available at www.ijraset.com*

Ninety-nine percent of exploited vulnerabilities have already been identified. Unfortunately, we have reliance on firewalls as a form of protection. Firewalls on the other hand will not affect the experienced hacker.[2] For the time being, humans are the only ones who try to predict what the other human will do before they can do it.[10]
Therefore, with this thought a few AI-based cyber security techniques are further discussed.

*1) AI based Cyber Threat Detection*

Cyberattacks have become more complicated and unpredictable than they have ever been. As a result, Artificial intelligence techniques are now being used in Cybersecurity systems. However, no AI model can be said to be 100 percent accurate.[8] As a result, incorrect predictions occur sometime requiring human intervention and response. However, keeping up with the continually growing number is becoming more challenging for human analysts.[3] Explainable Artificial Intelligence techniques have been developed to address such challenges. There are two aspects for this process.[11]
For developing a new model using a training dataset, the first step is to generate the Outlier score information which is a reliability indicator for AI prediction.[3] The shapely additive explanation model is then used to generate FOS information. It's based on how important each attribute is in AI's training data. [10]

2) *AI based counter measures for IoT network*

The Internet of Things (IoT) is one of the world's largest and fastest growing technologies. Securities worries around this network have grown in recent years. IoT devices are often considered as weak points and have become easy target for cyber-attacks.[6] AI-based solution with current conventional network protocol can be used to improve the security of IoT networks. The table 1 shows the various attacks in IoT environment.

Table 1: Types of cyber-attacks in IoT environment

| Attack Category | Attack Types |
|---|---|
| Probe | MS can, ports weep, Satan |
| UTR | SQL attack, root kit |
| R2L | Worm, imap |
| DOS | Udp storm, teardrop |

*3) Resilient ML for networked cyber – physical systems*

Many processes that previously required human intervention have been automated because of Cyber-Physical systems. It has gone a step further by being able to undertake control actions.[5] This has increased the risk of cyberattack by broadening the attack surface. This requires the use of resilient machine learning models.[12]

©IJRASET: All Rights are Reserved 

One of the most pressing concerns in CPS is the early detection of threats. This allows for the reduction of harm in the event of a cyberattack.[6] The use of machine learning techniques in the detection of assaults in CPS overcomes all of the drawbacks of state – space model like the Kalman filter.

Cybercriminals use several approaches to mislead the ML model to make incorrect classification.[19]
As a result, it is critical to make ML models themselves resistant to cyber-attacks. This can be accomplished in three ways: [8,9,10]

*a)* Adversarial Training: The purpose of this approach is to minimize the model's worst-case mistake when there is data anomaly during a cyberattack. It has a high success rate and makes the machine learning model resistant to attacks.
*b)* Randomization at Inference: Statistical method that calculates exact p-value and confidence intervals by analysing all possible permutations of treatment assignments in a randomized experiment rather than relying on large sample asymptotic assumptions.
*c)* Defensive distillation: It is a machine learning technique designed to increase the robustness of deep neural networks against adversarial network.[7] There are three primary processes in this procedure. The first is to train the network. Then it must be thoroughly analysed to obtain soft labels, another network is trained. This strategy is particularly good at generating a durable machine learning model.[5]

*4) Information theory techniques to detect cyber attack*

To avoid cyber-attack, it is important to understand the system and the steps that must be taken to protect it. This process requires a large number of datasets all of which are recording of previous data in a short amount of time.[4]
Normalizing the data sets is also a time-consuming process. Due to this issue the use of artificial intelligence security is extremely limited. To overcome these issues huge data sets must be shrunk increasing processing performance. This can be achieved by generating tiny sample sets.[11]
To address the previously mentioned issues information theory techniques might be incorporated into the earlier methodologies utilized by SROM models. The distribution changes are examined with time but remain constant within a window by employing information theory approaches.[7]

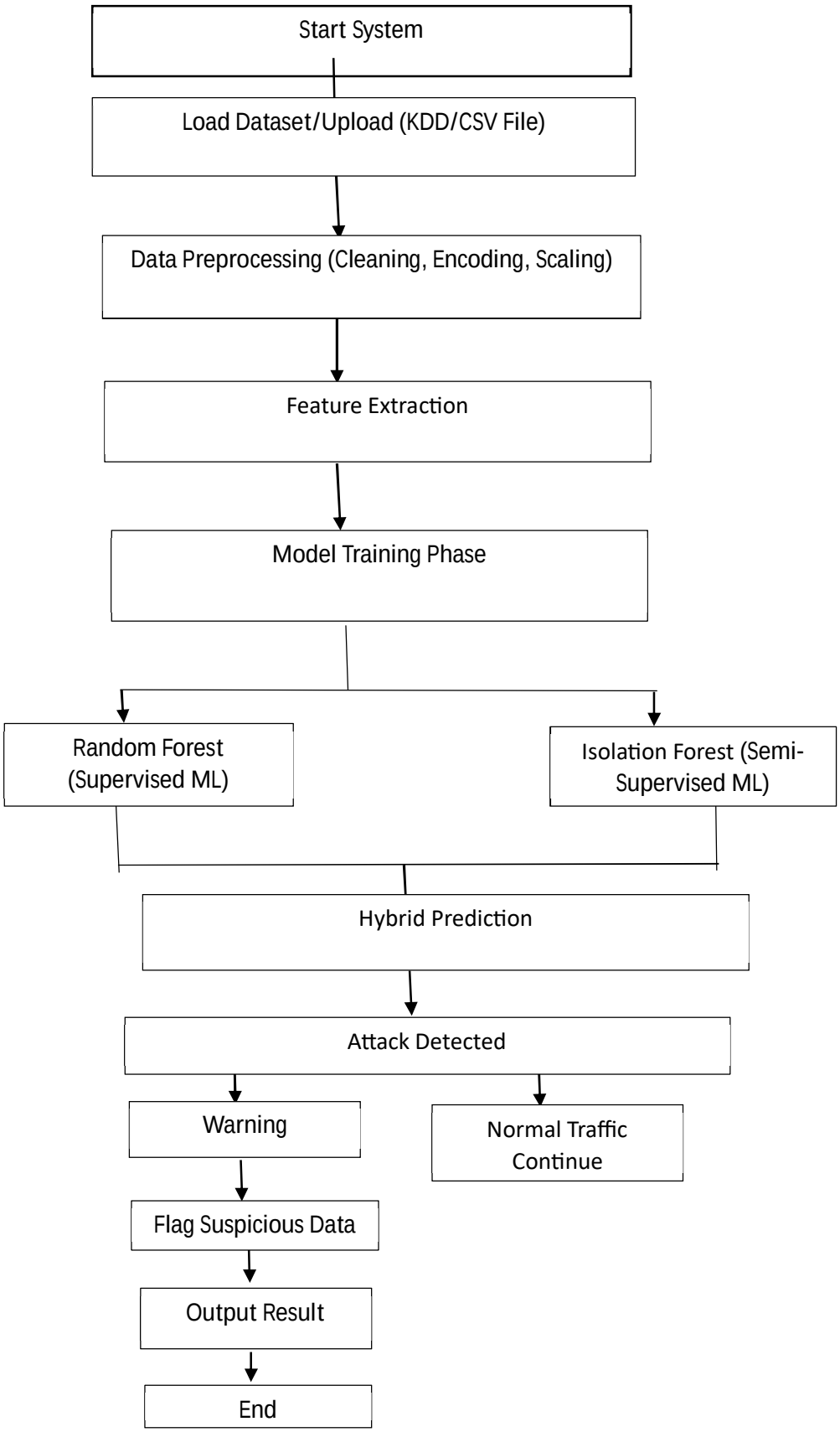
## II. LITERATURE REVIEW

AI-based cyber-attack detection and prevention systems represent a paradigm shift from reactive to proactive security, utilizing machine learning (ML) and deep learning (DL) to identify novel threats with higher accuracy and lower false positives.[20] Literature indicates that hybrid AI models combining anomaly-based detection with signature-based methods offer the best defence against complex, multi-stage and zero-day attacks.
Key AI techniques include SVM, Random Forest, LSTM for network traffic analysis, and Reinforcement Learning. However, challenges remain regarding high computational costs, dataset imbalance, and adversarial attacks targeting the AI itself.[8]
Cybersecurity has become major area of research because of increase in the number of experienced cyber-attacks.[11] Traditional Intrusion System are mainly classified into signature based and anomaly-based systems. Signature based system are effective for detecting known attack but fail to identify new threats or attacks.
On the other hand, Anomaly based systems can detect unknown attack but often suffer from high false positive rates.[8]
Recent research has focused on the use of Machine Learning (ML) and Deep Learning (DL) techniques to improve detection accuracy. Algorithms such as Decision tree, Random Forest, Support vector machine, and k-nearest neighbours (KNN) have been widely used for intrusion detection. Among these, Random Forest provides high accuracy and robustness, while SVM is effective in handling high dimensional data.
Deep learning models such as Artificial Neural Network (ANN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN) have also been explored for detecting complex attack patterns.[3] These models are capable of automatically extracting features from raw data, reducing the need for manual feature engineering. However, most system focus only on detection and lack an integrated prevention mechanism. This research addresses this limitation by combining AI-based detection with an automated prevention system, making it more practical and easier for real world applications.[19]

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue VI June 2026- Available at www.ijraset.com*

## III. PROPOSED SYSTEM ARCHITECTURE




©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

### A. *Data collection module*

This module collects network traffic data from various sources like system logs, network packets, or benchmark datasets like NSL-KDD and CICIDS. The collected data includes features like IP address, protocol types, packet sizes and connection duration. [16]

### B. *Data preprocessing module*

This module prepares the data for training by performing: [16]

- Data cleaning: It is a crucial preprocessing step that ensures the quality and reliability of the datasets. It involves identifying and removing inconsistencies such as missing values, duplicate records and noisy data.
- Feature selection: It is the process of identifying the most relevant attributes from the datasets that contribute to the prediction task. Redundant features are removed to reduced overfitting.
- Data normalization and scaling: It is used to bring all features value into a consistent range so that no single feature dominates the learning process due to its magnitude. Normalization rescales the value between 0 and 1 whereas standardization transforms data to have zero mean and unit variance. It is essential for algorithm like Support vector machine and Neural network as it improve convergence speed and model performance.

### C. *AI Detection Module*

This is the core module of the system. It uses Machine learning and Deep learning algorithm like:

Random Forest: It is based on machine learning algorithm that constructs multiple decision tree during training and result is based on majority voting by the multiple decision trees. It improves accuracy and reduces overfitting by combining the results of multiple trees.[11] In cybersecurity applications Random Forest is effective in handling large datasets and identifying complex attack pattern.

Decision function:

$$y\hat{}=\text{mode}\{T1(x), T2(x)..., Tn(x)\}$$

Where:

Ti(x) = prediction of the ithi^{th}ith decision tree

n = total number of trees

Support vector machine (SVM): It is a supervised machine learning algorithm used for classification and regression tasks. It works by finding an optimal hyperplane that separates data points of different classes with maximum margin.

Hyperplane equation:

$$w.x+b = 0$$

Where:

w = weight vector

x = input feature vector

b = bias

Kernel function (for non-linear cases):

$$K(xi, xj) = \phi(xi). \phi(xj)$$

Artificial Neural Network: It is a deep learning model inspired by the functioning of the human brain. It consists of the interconnected layers of neurons that process input data and learn complex patterns through training. It is widely used in cybersecurity for identifying experienced and new cyber-attacks.

Common activation functions are:

Sigmoid:

$F(x) = 1/1+e\hat{}-x$

Relu:

$F(x) = \max(0, x)$

Isolation Forest (Semi-supervised learning): It is an anomaly detection algorithm used to identify unknown or zero-day attacks. Unlike supervised models it does not require labelled data and work by isolating anomalies in the dataset. It is highly effective in detecting rare and unusual patterns in network traffic.

Decision function:

Anomaly Score(x) = Average path length in isolation trees.

This module classifies traffic into:

Normal traffic
Malicious traffic

*D. Prevention Module*

Once an attack is detected the module takes immediate action:

- Identifies and flags suspicious traffic for blocking and can be integrating with real-world firewall systems.
- Isolates infected systems
- Generates real-time alerts

*E. Database and Logging Module*

The module stores:

- Detected attack logs
- IP addresses
- Timestamp and attack types.

This data is useful for future analysis and reporting.

## IV. METHODOLOGY

The methodology of the proposed system is dived into the following steps: [14]

Step 1: Data Acquisition

The dataset is collected from standard sources such as NSL-KDD or CICIDS datasets.

Step 2: Data Preprocessing

- Remove missing values
- Convert categorical data into numerical form
- Normalize features

Step 3: Model Training

The system trains multiple models including:

- Random Forest
- Support Vector Machine
- Artificial Neural Network

These models learn patterns from labelled datasets.

Step 4: Attack detection

The trained model predicts whether incoming traffic is:

- Normal
- Malicious

Step 5: Prevention Mechanism

If malicious activity is detected:

- The IP is blocked
- Alerts are generated
- Logs are updated

*A. Hybrid detection Approach*

The proposed system combines predictions from random forest and isolation forest models. Random forest is used for detecting known attacks based on labelled data, while Isolation Forest identifies anomalous behaviour. The final decision is made using a hybrid rule, improving detection accuracy and robustness.[18]

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

## V. EXPERIMENTAL RESULT AND PERFORMANCE ANALYSIS

### *A. Performance Metrics*

To evaluate the performance of the proposed AI-based cyber-attack detection system several standard metrics are used. These metrics provide a comprehensive understanding of the model's effectiveness in detecting and classifying cyber-attacks. [19]

Accuracy: It calculates the overall correctness of the model by calculating the ratio of correctly predicted instances to the total number of instances.

Accuracy = TP+TN/TP+TN+FP+FN

Where:

TP = True Positive
TN = True Negative
FP = False Positive
FN = False Negative

Precision: It indicates the proportion of correctly identified attack instances among all instances predicted as attacks.

Precision = TP/TP+FP

Recall: It measures the model's ability to correctly detect all actual attack instances.

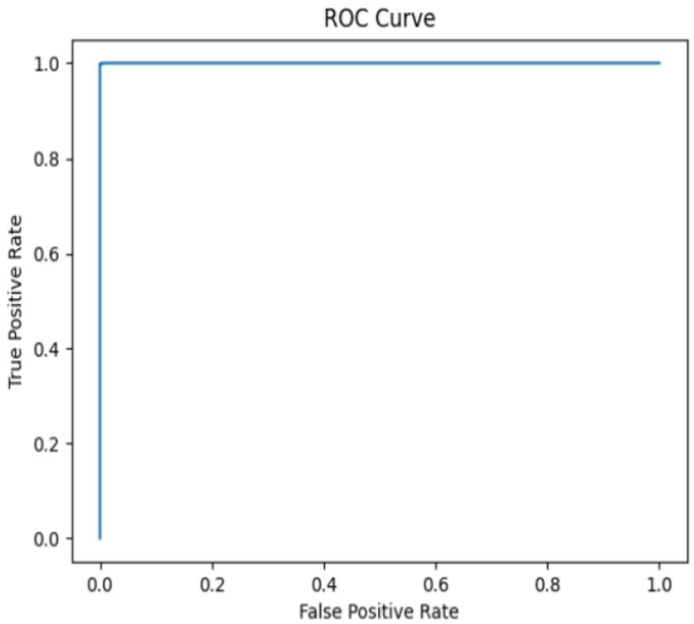
Recall = TP/TP+FN

F1-Score: It represents the harmonic mean of precision and recall providing a balance between two metrics.

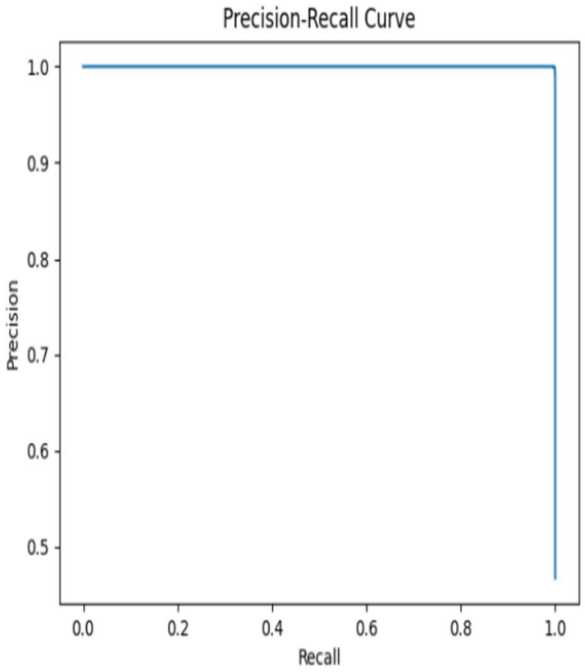
F1 = 2*PRECISION * RECALL/PRECISION + RECALL

### *B. Results and Graphs*

*1)* ROC CURVE

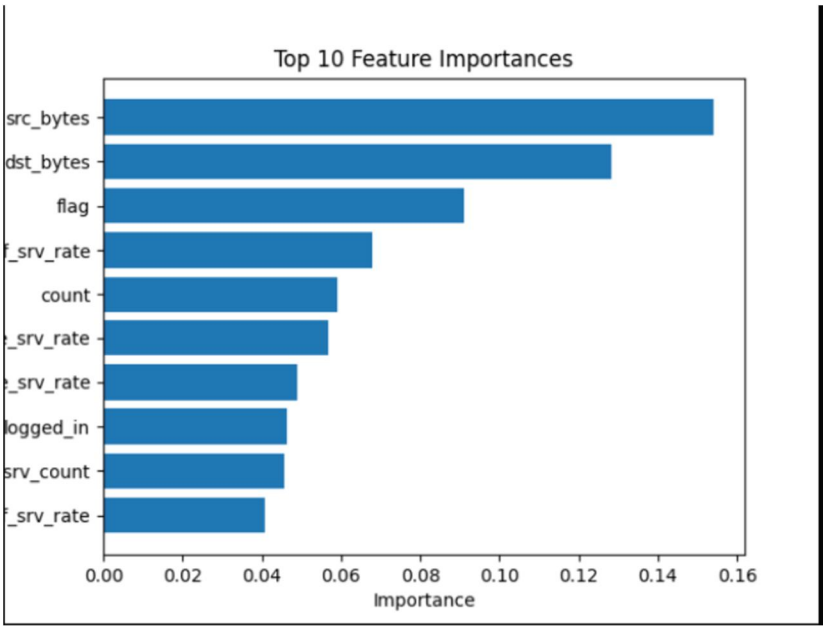


*2)* PRECISION – RECALL CURVE




This ROC curve illustrates the model's ability to distinguish between normal and malicious traffic, while the Precision-Recall curve highlights performance in handling imbalanced datasets. These results confirm the effectiveness of the hybrid model. The inclusion of the Isolation Forest model improves the system's ability to detect previously unseen attacks, while maintaining high precision and recall.

*C. Comparison Table*




©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*D. Performance Comparison Table*

| Model | Accuracy | Precision | Recall | F1-score |
|---|---|---|---|---|
| Random Forest | 95% | 94% | 96% | 95% |
| SVM | 92% | 91% | 93% | 92% |
| ANN | 96% | 95% | 97% | 96% |

The result show that the proposed AI- based system performs significantly better than traditional rule-based systems in terms of accuracy and detection capability.

## VI. CONCLUSION

This paper presents an AI-Based Cyber Attack Detection and Prevention System that enhances cybersecurity by applying intelligent detection and automated responses mechanism. The use of Machine Learning and Deep Learning techniques enables the system to detect both known and unknown cyber threats effectively. This inclusion of a prevention module further strengthens the system by enabling real time response to attacks.[20]

The experimental results demonstrate improved accuracy, reduced false positives, and faster response time compared to traditional method. Hence the proposed system provides a reliable and scalable solution for modern cybersecurity challenges.

The integration of semi-supervised learning improves the system's capability to detect unknown and zero-day attacks.[11] The simulated prevention module further enhances the practical applicability of the system in real-worlds cybersecurity environments.[14]

The hybrid learning approach combining supervised and semi-supervised techniques enhances the system's capability to detect both known and unknown cyber threats.[4]

## VII. FUTURE WORKS

The proposed system can be further enhanced in several ways to improve its real-world applicability and performance. Future works may focus on the following aspects:

*1)* Real – time deployment: Integrating the system with real-time network monitoring tools and packet capturing systems to enable live detection and prevention of cyber-attacks.[10]

*2)* Firewall and Intrusion Prevention Integration: Extending the simulated prevention module to a real-time prevention system by integrating with firewalls and intrusion prevention system (IPS) for automatic blocking of malicious traffic.[12]

*3)* Deep Learning models: Implementing advanced deep learning techniques such as convolutional neural network (CNN) and long short-term memory (LSTM) network to capture complex temporal and spatial patterns in network traffic.[11]

*4)* Explainable Artificial Intelligence (XAI): Incorporating explainability techniques to provide insights into model decision, helping security analyst understand why a particular activity is classified as malicious.[6]

*5)* Handling Encrypted Traffic: Enhancing the model to detect threats in encrypted network traffic without compromising data privacy.[19]

*6)* Scalability and Cloud Deployment: Deploying the system on cloud platform to handle large – scale network environments and high-volume data streams efficiently.[20]

*7)* Integration with SIEM Systems: Connecting the system with security information and event management (SIEM) tools for centralized monitoring, alerting and incident response.[17]

## REFERENCES

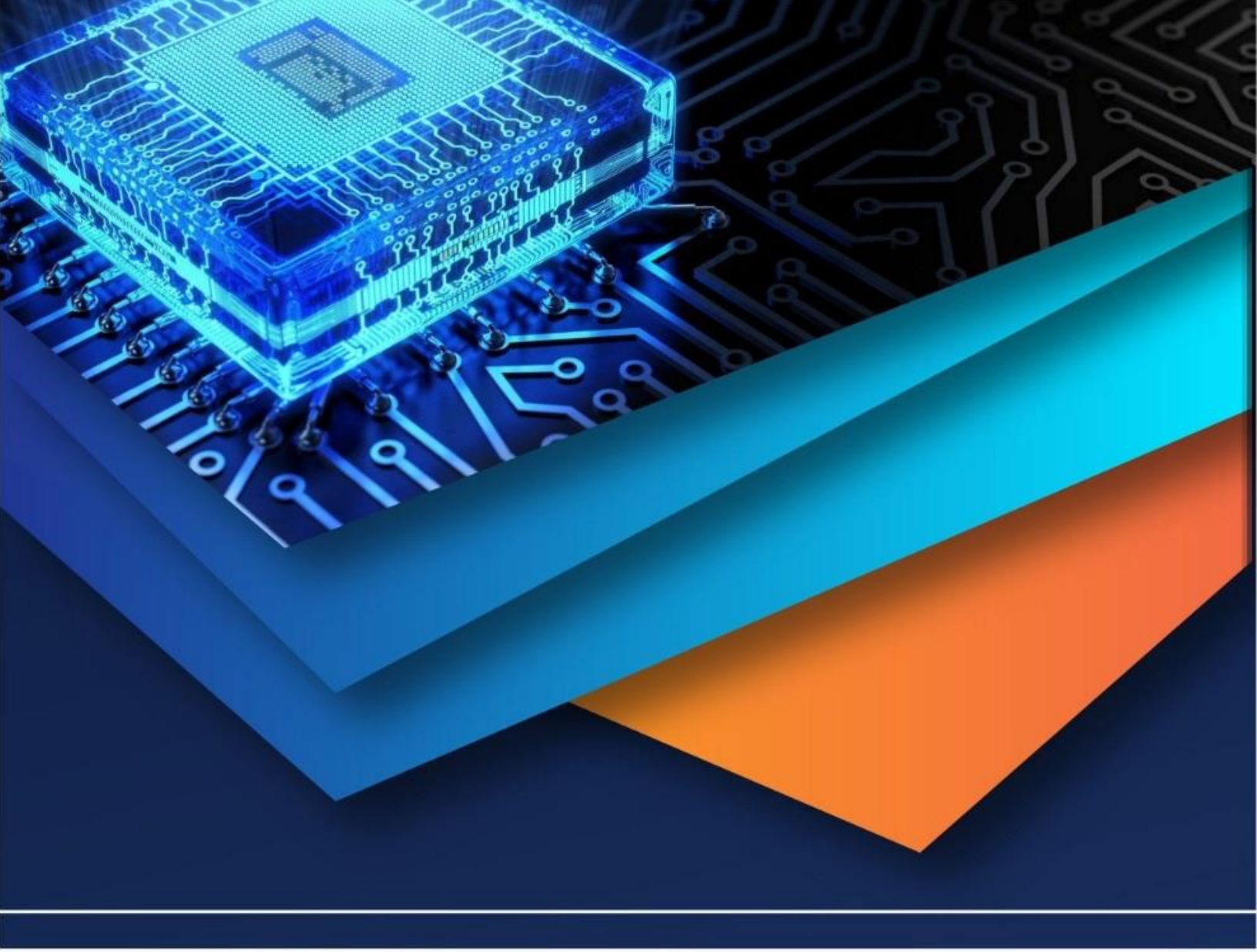
[1] Kandala kalyana Srinivas, et. al. International Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 12, Issue 6, (Series-V) June 2022, pp. 37-44.

[2] Kim, Y. Lee, E. Lee and T. Lee, &quote; Cost Effective Valuable Data Detection Based on the Reliability of Artificial Intelligence, & quote; in IEEE Access, vol. 9, pp. 108959-108974, 2021.

[3] X. Qiu, Z. Du and X. Sun, &quote; Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks, & quote; in IEEE Access, vol. 7, pp. 172004-172011, 2019, Doi: 10.1109/ACCESS.2019.2956480.

[4] X. Qiu, Z. Du and X. Sun, &quote; Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks, &quote; in IEEE Access, vol. 7, pp. 172004-172011, 2019, Doi: 10.1109/ACCESS.2019.2956480.
[5] F. Farivar, M. S. Haghighi, A. Jolfaei and M. Alazab, &quote; Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Hyperphysical Systems and Industrial IoT, &quote; in IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2716-2725, April 2020, Doi: 10.1109/TII.2019.2956474
[6] F. O. Olowononi, D. B. Rawat and C. Liu, &quote; Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS, &quote; in IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 524-552, First quarter 2021, Doi: 10.1109/COMST.2020.3036778
[7] B. Bordel, R. Alcarria, T. Robles and Á. Sánchez-Picot, &quote; Stochastic and Information Theory Techniques to Reduce Large Datasets and Detect Cyberattacks in Ambient Intelligence Environments, &quote; in IEEE Access, vol. 6, pp. 34896-34910, 2018, Doi: 10.1109/ACCESS.2018.2848100.
[8] Lee, J. Kim, I. Kim and K. Han, &quote; Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles, &quote; in IEEE Access, vol. 7, pp. 165607-165626, 2019, doi:10.1109/ACCESS.2019.2953095.
[9] B. Thuraisingham, &quote; Cyber Security and Artificial Intelligence for Cloud-based Internet of Transportation Systems, &quote; 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (Edgecomb), 2020, pp. 8-10, Doi: 10.1109/CSCloudEdgeCom49738.2020.00011.
[10] B. Thuraisingham, &quote; The Role of Artificial Intelligence and Cyber Security for social media, &quote; 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), 2020, pp. 1-3, doi:10.1109/IPDPSW50202.2020.00184.
[11] KANIMOZHI AND T.P. JACOB, &QUOTE; ARTIFICIAL INTELLIGENCE BASED NETWORK INTRUSION DETECTION WITH HYPER-PARAMETER OPTIMIZATION TUNING ON THE REALISTIC CYBER DATASET CSECIC-IDS2018 USING CLOUD COMPUTING, &QUOTE; 2019 INTERNATIONAL CONFERENCE ON COMMUNICATION AND SIGNAL PROCESSING (ICCSP), 2019, PP.0033-0036, DOI:10.1109/ICCSP.2019.8698029
[12] Sathya, J. Premalatha and S. Suwathika, &quote; Reinforcing Cyber World Security with Deep Learning Approaches, &quote; 2020 International Conference on Communication and Signal Processing (ICCSP), 2020, pp. 0766-0769, doi:10.1109/ICCSP48568.2020.9182067.
[13] Kuppala, K. K. Srinivas, P. Anudeep, R. S. Kumar and P. A. H. Vardhini, "Benefits of Artificial Intelligence in the Legal System and Law Enforcement," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 221-225, doi:10.1109/MECON53876.2022.9752352
[14] G. A. Chandra, K. K. Srinivas, P. Anudeep, S. R. Prasad, Y. Padmasai and P. Kishore, "Mental Health Disorder Analysis Using Convolution Neural Network Based Speech Signal Model with Integration of Artificial Intelligence," 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE), 2021, pp. 544-547, doi:10.1109/RDCAPE52977.2021.9633637.
[15] J. Kuppala, K. K. Srinivas, P. Anudeep, R. S. Kumar and P. A. H. Vardhini, "Benefits of Artificial Intelligence in the Legal System and Law Enforcement," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 221-225, doi:10.1109/MECON53876.2022.9752352.
[16] K. K. Srinivas, P. Vangara, R. Thiparapu, R. Sravanth Kumar and K. A. Bhagavathi, "Artificial Intelligence based Forecasting Techniques for the Covid-19 pandemic," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 297-301, doi:10.1109/MECON53876.2022.9752240.
[17] K. K. Srinivas, A. Peddi, S. K. Ramakuri, P. A. H. Vardhini, P. S. Avinash and R. Siri Malla, "Artificial Intelligence-Driven Techniques to Advanced Signals and Communication Systems," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 307-310, doi:10.1109/MECON53876.2022.9752011.
[18] Lee, J. Kim, I. Kim and K. Han, &quote; Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles, &quote; in IEEE Access, vol. 7, pp. 165607-165626, 2019, doi:10.1109/ACCESS.2019.2953095.
[19] N. Karennagari, K. Yashwanth Reddy, V. K. Gurrola, K. Srinivas, A. Peddi and Y. Padma Sai., "Infection Segmentation of Leaves Using Deep Learning techniques to enhance crop productivity in smart agriculture," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 368-372, doi:10.1109/ISPCC53510.2021.9609379.
[20] G. A. Chandra, K. K. Srinivas, P. Anudeep, S. R. Prasad, Y. Padmasai and P. Kishore, "Mental Health Disorder Analysis Using Convolution Neural Network Based Speech Signal Model with Integration of Artificial Intelligence," 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE), 2021, pp. 544-547, doi:10.1109/RDCAPE52977.2021.9633637.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)