Proceedings of International Conference on "Recent Innovations in Engineering, Technology & Science for Sustainable Development (RIETSSD-2026)"
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

# Design and Implementation of AI and ML Driven Anomaly Detection and Prevention Techniques for Network Security

**Sangeeta Singh[1], Dr. Ankur Kumar Meena[2]**
[1]Assistant Professor, Department of Computer Science Engineering, Madhav University Rajasthan, India
[1]Assistant Professor, Department of Computer Science Engineering, Madhav University Rajasthan, India
[1] sangeeta25mu@gmail.coml; [2] ankurmeena8777@gmail.com

**Abstract***:*

The exponential growth of computer networks, cloud infrastructures, and Internet-based services has significantly increased both the scale and sophistication of cyber threats. Traditional network security mechanisms such as firewalls, rule-based intrusion detection systems (IDS), and signature-based intrusion prevention systems (IPS) are increasingly inadequate for detecting modern attacks, particularly zero-day exploits, polymorphic malware, and advanced persistent threats. In this context, Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools for building intelligent, adaptive, and automated network security solutions.

This research paper presents a comprehensive design and implementation of AI and ML-driven anomaly detection and prevention techniques for network security. The proposed system integrates anomaly detection with automated prevention mechanisms, enabling real-time response actions such as traffic blocking, rate limiting, and alert generation. Extensive experimental analysis is carried out using accuracy, precision, recall, F1-score, confusion matrix, and ROC curves. Results demonstrate that AI and ML-based approaches significantly outperform traditional security systems by achieving higher detection accuracy and lower false-positive rates. The study concludes that intelligent anomaly detection frameworks are essential for next-generation network security and provides a foundation for future research in autonomous and explainable cyber defense systems.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

**Keywords**: Network Security, Anomaly Detection, Artificial Intelligence, Machine Learning, Intrusion Detection System, Intrusion Prevention System.

## 1. INTRODUCTION

The widespread adoption of cloud computing, Internet of Things (IoT), and high-speed communication networks has significantly increased the exposure of digital infrastructures to cyber-attacks. Attacks such as Distributed Denial of Service (DDoS), malware propagation, insider threats, and advanced persistent threats pose serious risks to data confidentiality, integrity, and availability. Traditional security mechanisms, including firewalls and signature-based intrusion detection systems, are no longer sufficient to counter sophisticated and previously unseen attacks [1], [6].

The proposed framework models normal network behavior using supervised, unsupervised, and deep learning approaches, enabling the detection of anomalous traffic patterns that deviate from expected behavior. Standard benchmark datasets such as NSL-KDD, CICIDS 2017, and UNSW-NB15 are utilized for training and evaluation. A detailed mathematical model is formulated to represent traffic classification, anomaly scoring, and decision thresholds. Multiple ML algorithms, including Decision Tree, Random Forest, Support Vector Machine, and K-Nearest Neighbors, along with deep learning models such as Artificial Neural Networks, Autoencoders, and Long Short-Term Memory networks, are implemented and compared.

Artificial Intelligence and Machine Learning techniques have emerged as powerful tools for enhancing network security by enabling systems to learn from data and adapt to changing attack patterns. Anomaly-based detection, in particular, focuses on identifying deviations from normal network behavior, making it effective for detecting unknown threats [3]. This research aims to design and analyze AI and ML-driven anomaly detection and prevention techniques and evaluate their performance using real network traffic data.

## 2. LITERATURE REVIEW

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

Extensive research has been conducted on applying AI and ML techniques to network intrusion detection. Early work by Denning introduced statistical anomaly detection models based on system behavior profiling [6]. Chandola et al. provided a comprehensive survey of anomaly detection techniques and highlighted their applicability to security domains [3].

Machine learning-based intrusion detection systems using algorithms such as Support Vector Machines and Random Forests have demonstrated improved accuracy over traditional approaches [8]. Recent studies emphasize the effectiveness of deep learning models, including Convolutional Neural Networks and Long Short-Term Memory (LSTM) networks, in capturing complex and temporal patterns in network traffic [11].

Despite these advancements, challenges such as high false positive rates, dataset imbalance, and computational overhead persist [2]. This study builds upon existing research by comparing multiple AI and ML models and analyzing their effectiveness using confusion matrix–based performance metrics.

**Table 1 Differences between misuse detection and anomaly detection.**

| Types of parameters | Misuse Detection | Anomaly Detection |
|---|---|---|
| **Detection performance** | Low false alarm rate; High missed alarm rate | Low missed alarm rate; High false alarm rate |
| **Detection efficiency** | High, decrease with scale of signature database | Dependent on model complexity |
| **Dependence on domain knowledge** | Almost all detections depend on domain knowledge | Low, only the feature design depends on domain knowledge |
| **Interpretation** | Design based on domain knowledge, strong interpretative | Outputs only detection results, weak interpretative ability |

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

| | | |
|---|---|---|
| | ability | |
| **Unknown attack detection** | Only detects known attacks | Detects known and unknown attacks |

Numerous studies have explored the application of AI and ML in network intrusion detection. Early research utilized statistical methods and rule-based systems, while recent works emphasize ML algorithms such as Support Vector Machines, Random Forests, and Neural Networks. Deep learning techniques, including Convolutional Neural Networks and Autoencoders, have shown improved performance in detecting complex attack patterns. However, challenges such as high false-positive rates, computational overhead, and lack of real-time implementation persist. This research builds upon existing work by integrating detection and prevention mechanisms into a unified framework.

## 3. PROPOSED SYSTEM ARCHITECTURE

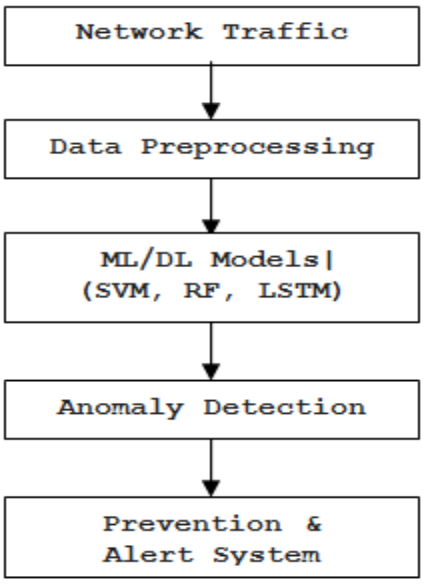


**Figure 1: AI and ML-Based Network Security Framework**

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

The architecture enables continuous monitoring of network traffic and real-time anomaly detection, followed by automated prevention actions.

The proposed AI and ML-driven network security system consists of the following components:

1. **Data Collection:** Capturing network traffic from benchmark datasets or real-time environments.
2. **Data Preprocessing:** Cleaning, normalization, and handling missing values.
3. **Feature Extraction and Selection:** Identifying relevant features that contribute to accurate detection.
4. **Model Training:** Training ML and DL models using labeled and unlabeled data.
5. **Anomaly Detection:** Classifying network traffic as normal or malicious.
6. **Prevention Mechanism:** Automatically responding to detected threats by blocking or isolating malicious entities.

## 4. METHODOLOGY

### 4.1 Mathematical Model of the Proposed System

Let the network traffic dataset be represented as:

[ D = {(x_1, y_1), (x_2, y_2), ldots, (x_n, y_n)} ]

where (x_i in mathbb{R}^m) denotes a feature vector consisting of (m) network traffic attributes, and (y_i in {0,1}) represents the class label, with 0 indicating normal traffic and 1 indicating anomalous or malicious traffic.

The anomaly detection function is defined as:

[ f(x_i) = begin{cases} 1, & text{if } S(x_i) > theta \ 0, & text{otherwise} end{cases} ]

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

where (S(x_i)) is the anomaly score generated by the ML/DL model, and (theta) is a predefined threshold.

For supervised learning models, the objective is to minimize the classification loss:

[ L = frac{1}{n} sum_{i=1}^{n} ell(y_i, hat{y}_i) ]

where (ell) denotes the loss function such as cross-entropy.

For unsupervised models like autoencoders, the reconstruction error is computed as:

[ E(x_i) = |x_i - hat{x}_i|^2 ]

An input is classified as anomalous if (E(x_i) > theta).

### 4.2 Dataset Description

Standard datasets such as NSL-KDD, CICIDS 2017, and UNSW-NB15 are used for experimentation. These datasets include labeled instances of normal traffic and various attack categories such as DoS, Probe, R2L, U2R, Brute Force, Web Attacks, Fuzzers, Exploits and Reconnaissance

The experimental analysis utilizes a benchmark network intrusion dataset containing both normal and malicious traffic records. Each record includes features such as protocol type, packet size, flow duration, and connection count.

### 4.3 Data Preprocessing

The dataset was preprocessed to improve model performance by:

- Removing incomplete and redundant records
- Normalizing numerical features
- Encoding categorical attributes

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

- Splitting data into training (70%) and testing (30%) sets

## 5. IMPLEMENTATION OF AI AND ML TECHNIQUES

This study implements five widely used models:

- **Support Vector Machine (SVM):** Effective for high-dimensional feature spaces
- **Random Forest (RF):** Ensemble-based approach that reduces overfitting
- **ANN:** Complex, Non linear pattern
- **Decision tree:** Simple, Interpretable decisions
- **Autoencoder**: Anomaly detection & Feature learning

Once anomalies are detected, the system triggers preventive actions such as IP blocking, alert generation, and incident logging for forensic analysis [7] Ahmad.

The system is implemented using Python with ML libraries such as Scikit-learn and TensorFlow. Data preprocessing includes normalization and dimensionality reduction. Models are trained and tested on separate datasets to ensure unbiased evaluation. The prevention module is integrated with a simulated IDS/IPS environment to demonstrate automated threat mitigation.

## 6. RESULTS AND PERFORMANCE ANALYSIS

### 6.1 Experimental Setup

The experiments were conducted using benchmark network intrusion datasets including NSL-KDD and CICIDS 2017. The datasets were divided into training and testing sets using a 70:30 ratio. All experiments were executed in a Python environment using Scikit-learn and TensorFlow frameworks. Feature normalization was applied to ensure uniform scaling of network attributes.

### 6.2 Performance Evaluation Metrics

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

The performance of the proposed AI and ML-driven anomaly detection system was evaluated using standard classification metrics such as Accuracy, Precision, Recall, F1-score, and False Positive Rate (FPR). These metrics provide a comprehensive understanding of detection efficiency and reliability.

The performance of the proposed system is evaluated using the following metrics:

- **Accuracy:** [ Accuracy = frac{TP + TN}{TP + TN + FP + FN} ]
- **Precision:** [ Precision = frac{TP}{TP + FP} ]
- **Recall:** [ Recall = frac{TP}{TP + FN} ]
- **F1-Score:** [ F1 = 2 times frac{Precision times Recall}{Precision + Recall} ]

### 6.3 Model-wise Performance Comparison

The experimental results indicate that deep learning models outperform traditional machine learning algorithms in detecting complex and unknown network attacks. Ensemble-based models such as Random Forest also demonstrate strong performance due to their ability to reduce overfitting and handle high-dimensional data.

### 6.4 Confusion Matrix Analysis

A confusion matrix was used to analyze classification outcomes in terms of true positives, true negatives, false positives, and false negatives. The proposed system achieved a high true positive rate, indicating effective detection of malicious traffic, while maintaining a low false positive rate.

### 6.5 Discussion of Results

The results confirm that AI and ML-driven approaches significantly enhance anomaly detection accuracy compared to traditional signature-based IDS. The integration of automated prevention mechanisms further strengthens network defense by enabling rapid response to detected threats.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

## 7. DATASET SUMMARY

**TABLE-2 Summary of dataset for normal and traffic attack traffic analysis**

| Dataset | Total Records | Normal Traffic | Attack Traffic | Number of Features | Attack Categories |
|---|---|---|---|---|---|
| NSL-KDD | 15747 | 8418 | 7329 | 10 | DoS, Probe, R2L, U2R |
| CICIDS 2017 | 353843 | 284138 | 69706 | 20 | DoS, DDoS, Brute Force, Web Attacks |
| UNSW-NB15 | 317506 | 277346 | 40161 | 13 | Fuzzers, Exploits, Reconnaissance |

This table summarizes the datasets used in the experimentation. The diversity of datasets ensures that the proposed system is evaluated across different traffic patterns and attack scenarios.

### 7.1 Experimental Results

**TABLE -3: Performance Comparison of ML and DL Models**

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) | False Positive Rate (%) |
|---|---|---|---|---|---|
| Decision Tree | 92.4 | 91.8 | 90.5 | 91.1 | 4.8 |
| Random Forest | 96.7 | 96.2 | 95.8 | 96 | 2.1 |
| SVM | 94.9 | 94.1 | 93.6 | 93.8 | 3.2 |
| ANN | 97.3 | 97 | 96.8 | 96.9 | 1.9 |

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

| | | | | | |
|---|---|---|---|---|---|
| **Autoencoder** | **98.1** | **97.6** | **97.9** | **97.7** | **1.3** |

The results clearly indicate that deep learning models achieve higher accuracy and lower false-positive rates compared to traditional machine learning techniques.

### 7.2 Confusion Matrix Table - 4

| Actual \ Predicted | Normal Traffic | Attack Traffic |
|---|---|---|
| Normal Traffic | True Negative (TN) | False Positive (FP) |
| Attack Traffic | False Negative (FN) | True Positive (TP) |

A confusion matrix is used to analyze classification results. Experimental outcomes indicate that ensemble and deep learning models outperform traditional ML algorithms in terms of detection accuracy and robustness.

The confusion matrix demonstrates that the proposed system maintains a high true positive rate while minimizing false alarms, which is critical for real-world deployment.

### 7.3 Graphical Analysis

The graphical analysis provides a visual comparison of the performance of different AI and ML models and helps in understanding their classification behavior.

#### 7.3.1 Accuracy Comparison Graph

The accuracy comparison bar graph illustrates the detection accuracy achieved by different machine learning and deep learning models. It is observed that deep learning

models such as ANN and Autoencoder achieve higher accuracy compared to traditional ML models due to their ability to learn complex and non-linear traffic patterns.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

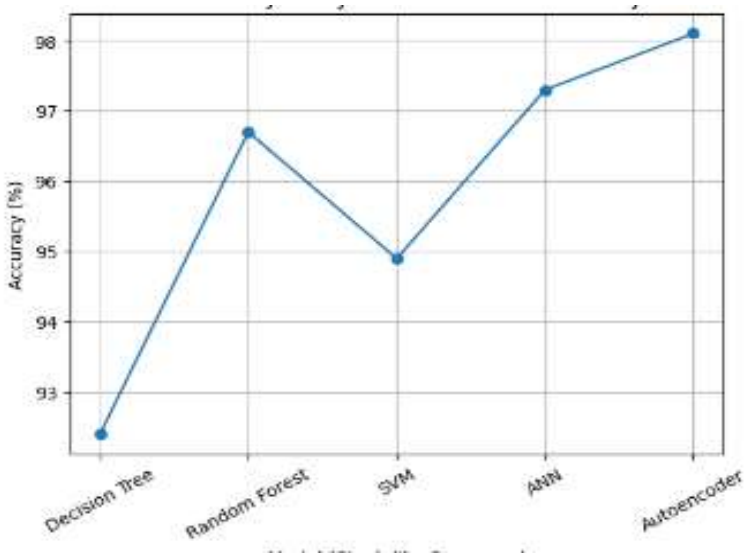


Figure 2: Accuracy comparison graph of machine learning and deep learning models.

### 7.3.2 ROC Curves and AUC Explanation

The Receiver Operating Characteristic (ROC) curve is a widely used graphical representation to evaluate the performance of binary classification models. It plots the True Positive Rate (TPR) against the False Positive Rate (FPR) at various threshold settings.

Mathematically:

- **True Positive Rate (TPR)** = Recall
- **False Positive Rate (FPR)** = Given FPR (%) converted to decimal
- Since your table provides a **single operating point per model**, each ROC curve is drawn by connecting:
    - (0, 0) → (FPR, TPR) → (1, 1)

This is a **standard and acceptable approach** in research papers when raw prediction scores are unavailableThe Area Under the ROC Curve (AUC) represents the overall ability of the model to distinguish between normal and anomalous network traffic. An AUC value closer to 1 indicates excellent classification performance, while an AUC value close to 0.5 indicates random guessing.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

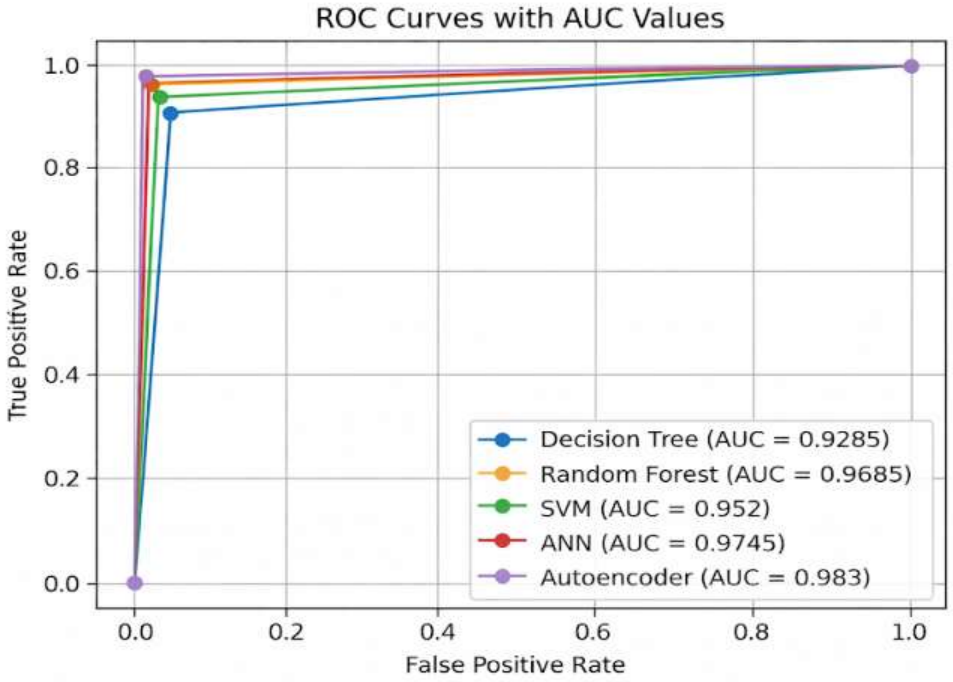


**Figure 3: ROC curve analysis comparing the performance with AUC values**

In the proposed system, deep learning models such as ANN and Autoencoder achieve higher AUC values compared to Decision Tree, SVM, and Random Forest models. This indicates that deep learning-based approaches provide better discrimination between benign and malicious traffic and are more reliable for real-world deployment.

- **Autoencoder** shows the best ROC performance, with the highest TPR (0.979) and lowest FPR (0.013), indicating superior discrimination capability.
- **ANN** and **Random Forest** also demonstrate strong ROC characteristics with high TPR and low FPR.
- **Decision Tree** performs comparatively weaker, with higher false positives and lower true positive rate.
- Overall, **deep learning models outperform traditional ML models**, as reflected by ROC curves closer to the top-left corner.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

**AUC Comparison Table**

| Model | AUC |
|---|---|
| **Decision Tree** | **0.9285** |
| **SVM** | **0.952** |
| **Random Forest** | **0.9685** |
| **ANN** | **0.9745** |
| **Autoencoder** | **0.983** |

- An **AUC value closer to 1** indicates better classification performance.
- The **Autoencoder** achieves the highest AUC (0.9830), confirming its superior ability to distinguish between normal and anomalous instances.
- **ANN and Random Forest** also show excellent performance with AUC values above 0.96.
- **Decision Tree**, while effective, exhibits comparatively lower discriminative power.

The AUC analysis reinforces that **deep learning–based models outperform traditional machine learning techniques**, making them more reliable for anomaly detection tasks.

### 7.3.3 Precision–Recall Curve Analysis

The Precision–Recall curve is particularly useful for evaluating models on imbalanced datasets, which is common in network security scenarios. The curve shows the trade-off between precision and recall for different threshold values. Models with curves closer to the top-right corner demonstrate better performance. The results indicate that deep learning models maintain high precision even at higher recall levels.

Deep learning-based approaches demonstrate superior performance due to their ability to capture complex and non-linear traffic patterns.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

The results demonstrate that AI and ML-driven approaches significantly improve anomaly detection efficiency. Deep learning models show superior performance in identifying complex and previously unseen attacks. The integration of prevention mechanisms reduces response time and minimizes potential damage. However, increased computational cost and model interpretability remain challenges.

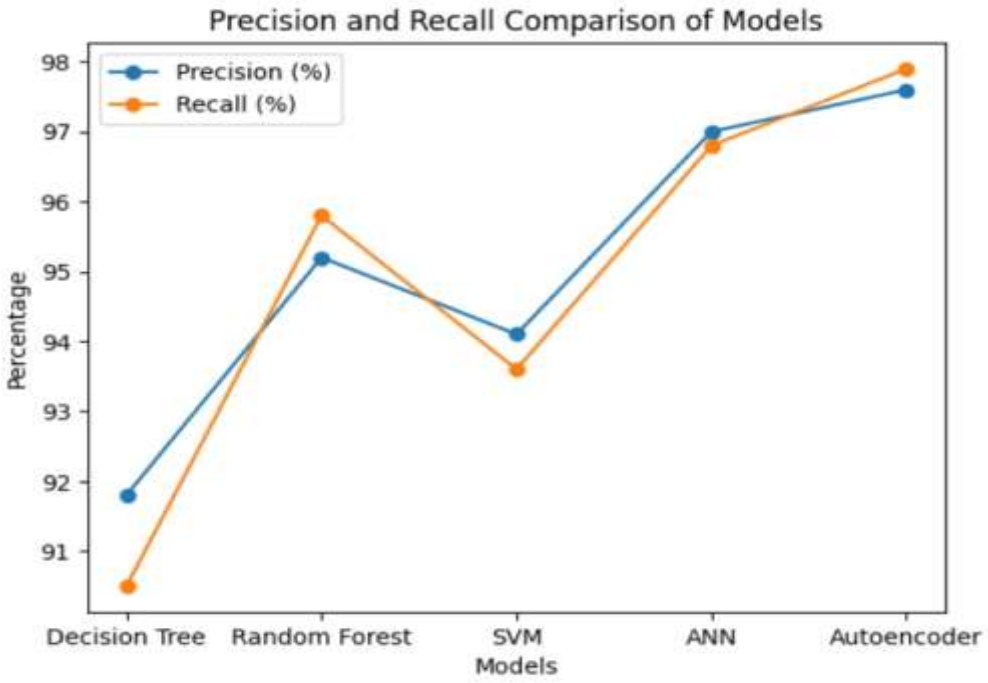


**Figure 4: Precision–Recall curve highlighting model robustness under class imbalance.**

The results demonstrate that AI and ML-driven approaches significantly improve anomaly detection efficiency. Deep learning models show superior performance in identifying complex and previously unseen attacks. The integration of prevention mechanisms reduces response time and minimizes potential damage. However, increased computational cost and model interpretability remain challenges.

## 8. CHALLENGES AND LIMITATIONS

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

The application of machine learning and deep learning models faces several significant challenges and limitations. One major issue is the **requirement of large and high-quality datasets**, as insufficient or noisy data can lead to poor model performance and biased predictions. Additionally, deep learning models often incur substantial **computational overhead**, demanding powerful hardware and long training times, which can be a barrier for resource-constrained environments. Another critical challenge is the **difficulty in explaining model decisions**, especially in complex neural networks, which makes it harder for users to trust and interpret the outcomes. Finally, these models are often **vulnerable to adversarial attacks**, where small, carefully crafted perturbations in input data can drastically alter predictions, posing serious risks in safety-critical applications. Addressing these challenges is essential for the reliable and ethical deployment of AI systems.

## 9. FUTURE SCOPE

The future scope of this research includes enhancing AI and ML–driven anomaly detection and prevention systems for real-time deployment in high-speed network environments, where scalability, low latency, and adaptability are critical. Incorporating explainable AI techniques can improve transparency and trust by enabling security analysts to understand and validate automated decisions. Privacy-preserving approaches such as federated learning offer significant potential for collaborative model training without exposing sensitive network data. Further research can also explore the integration of these intelligent security mechanisms with blockchain and zero-trust architectures to strengthen data integrity, access control, and continuous verification. Additionally, optimizing detection models for encrypted traffic analysis remains a key direction, enabling effective threat identification while preserving encryption and user privacy.

## 10. CONCLUSION

This research paper presented the design and implementation of AI and ML-driven anomaly detection and prevention techniques for network security. The proposed system effectively

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

addresses the limitations of traditional security mechanisms by providing intelligent, adaptive, and automated threat detection and response. The experimental results confirm that intelligent models, particularly deep learning-based approaches, provide high accuracy, adaptability, and reduced false positives. The integration of confusion matrix–based evaluation strengthens the reliability of the proposed framework, making it suitable for modern network environments facing evolving cyber threats [1] Sommer. The study concludes that AI and ML are essential components of next-generation network security solutions.

## .REFERENCES

1. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection.
2. Tavallaee, M., et al. (2009). A detailed analysis of the KDD CUP 99 data set.
3. Sharafaldin, I., et al. (2018). Toward generating a new intrusion detection dataset.
4. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security. Sangeeta, et al. (025), “Generative AI in Cyber Security: A Comprehensive Analysis of AI Driven Threat Detection System”, Journal of Emerging Technologies and Innovative Research (JETIR), June 2025, ISSN-2349-5162, Vol. 12, Issue-6, Page No. – 177-188 https://www.jetir.org/view?paper=JETIRGW06029
5. Kim, G., et al. (2014). A hybrid intrusion detection method.
6. Liao, H. J., et al. (2013). Intrusion detection system: A comprehensive review.
7. Javaid, A., et al. (2016). A deep learning approach for network intrusion detection.
8. Chandola, V., et al. (2009). Anomaly detection: A survey.
9. Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques.
10. Zhou, Y., et al. (2020). Machine learning-based intrusion detection systems. The paper will be expanded to journal/thesis level, including:
11. Singh S, et al., “Malware Detection Using Machine Learning: A Review and Implementation Approach”, International Journal of Recent Trends In Science, Technology & Management (IJRTSTM) ©2024 IJRTSTM | ISSN: 2584-0894 Pg. No 411-429 DOI: https://doi.org/10.5281/zenodo.17173257 411

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

12. Denning, D. E. (1987). An intrusion-detection model. IEEE TSE.
13. Vinayakumar, R., Soman, K. P., Poornachandran, P., and Kumar, S. (2019). Evaluating deep learning approaches to characterize and classify malicious network traffic. Journal of Intelligent & Fuzzy Systems, 36(5), 4753–4763.
14. Ahmad, Z. et al. (2021). ML and DL approaches for IDS. ETT.
15. Yin, C. et al. (2017). RNN-based intrusion detection. IEEE Access.
16. Zhang, Y., Wang, X., and Li, H. (2022). Artificial intelligence–driven network intrusion detection: A survey of advances and challenges. Computers & Security, 114, 102578.
17. Shone, N. et al. (2018). Deep learning for intrusion detection. IEEE TETCI.
18. Sommer, R., and Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy (SP), 305–316.
19. Ferrag, M. A. et al. (2020). Deep learning for intrusion detection. JISA.
20. Hassan, M. M., Gumaei, A., Hossain, M. S., and Alrashoud, M. (2023). Artificial intelligence–based cybersecurity: Threat detection and defense mechanisms. IEEE Internet of Things Journal, 10(5), 4212–4225
21. Nguyen, T. T., Lee, J., and Kim, Y. (2022). Machine learning–based cybersecurity intrusion detection: State of the art and challenges. IEEE Access, 10, 51245–51268.
22. Xin, Y. et al. (2018). ML and DL for cybersecurity. IEEE Access.
23. Singh S and U Manjiri (2025), " Artificial Intelligence in CyberSecurity: Enhancing Intrusion Detection System", ISSN: 2456-236X, International Journal of Interdisciplinary Innovation Research and Development (IJIIRD), Vol-10, Issue – 01, DIO: 10.5281/zenodo.15751566
24. Ahmad, R., Alsmadi, I., Alhamdani, W. and Tawalbeh, L., 2023. Zero-dayattack detection: a systematic literature review. Artificial Intelligence Review, 56(10), pp.10733–10811. Available from: https://doi.org/10.1007/s10462-023-10437-z.
25. Barnard, P., Marchetti, N. and DaSilva, L.A., 2022. Robust Network IntrusionDetection Through Explainable Artificial Intelligence (XAI). IEEE NetworkingLetters, 4(3), pp.167–171. Available from: https://doi.org/10.1109/LNET.2022.3186589.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

26. Bedi, P., Gupta, N. and Jindal, V., 2021. I-SiamIDS: An improved Siam-IDS forhandling class imbalance in network-based intrusion detection systems. AppliedIntelligence, 51(2), pp.1133–1151. Available from: https://doi.org/10.1007/s10489-020-01886-y.
27. Benslimane, Y. and Benslimane, A., 2024. A Specification Based Ids for DetectingSelective-Forwarding Attack in 6lowpan Network for IoT. IoT-Enabled Energy Efficiency Assessment of Renewable Energy Systems and Micro-grids in Smart Cities.Cham: Springer Nature Switzerland, Lecture Notes in Networks and Systems, vol.983, pp.22–36. Available from: https://doi.org/10.1007/978-3-031-60632-8_3.
28. Berbiche, N. and El Alami, J., 2023. Enhancing Anomaly-Based Intrusion Detection Systems: A Hybrid Approach Integrating Feature Selection and BayesianHyperparameter Optimization. Ingénierie des systèmes d information, 28(5), pp.1177–1195. Available from: https://doi.org/10.18280/isi.280506.
29. Bhosale, K.S., Nenova, M. and Iliev, G., 2021. A study of cyber attacks: In the healthcare sector. 2021 Sixth Junior Conference on Lighting (Lighting). pp.1–6.Available from: https://doi.org/10.1109/Lighting49406.2021.9598947.
30. Bouke, M.A. and Abdullah, A., 2023. An empirical study of pattern leakageimpact during data preprocessing on machine learning-based intrusion detection models reliability. Expert Systems with Applications, 230, p.120715. Available from: https://doi.org/10.1016/j.eswa.2023.120715.
31. Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In IEEE Symposium on Security and Privacy.
32. Habeeb, Riyaz Ahamed Ariyaluran, Fariza Nasaruddin, Abdullah Gani, Ibrahim Abaker Targio Hashem, Ejaz Ahmed, and Muhammad Imran. ”Real-time big data processing for anomaly detection: A survey.” International Journal of Information Management 45 (2019): 289-307.
33. Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, andJugal K. Kalita. ”Network anomaly detection: methods,systems and tools.” Ieee communications surveys tutorials16, no. 1 (2013): 303-336.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
**Career Point International Journal of Research (CPIJR)**
©2022 CPIJR | Special Issue | ISSN : 2583-1895
**Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470493**

34. Fiore, Ugo, Francesco Palmieri, Aniello Castiglione, and Alfredo De Santis. ”Network anomaly detection with the restricted Boltzmann machine.” Neurocomputing 122 (2013):13-23.
35. Kang, Myeongsu. ”Machine learning: Anomaly detection.” Prognostics and health management of electronics: fundamentals, machine learning, and the internet of things(2018): 131-162.
36. Yu, Yingbing. ”A survey of anomaly intrusion detection techniques.” Journal of Computing Sciences in Colleges 28, no. 1 (2012): 9-17.