International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Hybrid Artificial Intelligence Framework for Early Detection and Prevention of Cyber Threats

[1]Subhalaxmi Nayak, [2]Rumana Hasinullah Shaikh

[1],[2] Department of Computer Science Engineering ,GIFT Autonomous ,Bhubaneswar,

Abstract - The rapid growth of digital communication systems, cloud computing, Internet of Things (IoT), and online platforms has significantly increased cybersecurity threats. Traditional security mechanisms are often unable to detect sophisticated cyberattacks such as ransomware, phishing, malware, and Distributed Denial of Service (DDoS) attacks in real time. Artificial Intelligence (AI) provides intelligent and automated solutions for identifying suspicious activities and preventing cyber threats. This paper proposes a Hybrid Artificial Intelligence Framework that combines Machine Learning (ML), Deep Learning (DL), and rule-based systems for the early detection and prevention of cyber threats. The proposed framework integrates anomaly detection, behavioral analysis, and predictive analytics to improve cybersecurity performance. Experimental analysis demonstrates that hybrid AI models achieve higher detection accuracy, faster response time, and reduced false positives compared to traditional cybersecurity systems.

Keywords— Artificial Intelligence, Cybersecurity, Machine Learning, Deep Learning, Threat Detection, Intrusion Detection System, Hybrid AI Framework.

I. INTRODUCTION

The advancement of digital technologies has transformed modern society by enabling online communication, cloud services, e-commerce, smart devices, and remote computing. However, the rapid growth of interconnected systems has also increased cybersecurity risks. Cyberattacks such as phishing, ransomware, spyware, botnets, and DDoS attacks threaten organizations, governments, and individuals worldwide.

Traditional cybersecurity approaches mainly depend on predefined signatures and manual analysis techniques. These methods are not effective against advanced persistent threats and zero-day attacks because attackers continuously modify attack patterns. Therefore, intelligent and adaptive cybersecurity solutions are necessary.

Artificial Intelligence (AI) enables systems to analyze large amounts of network data, recognize attack patterns, and automatically respond to malicious activities. Hybrid AI combines multiple AI techniques such as Machine Learning, Deep Learning, and expert systems to improve cybersecurity performance.

This paper presents a Hybrid Artificial Intelligence Framework for early detection and prevention of cyber threats. The framework improves security accuracy, reduces false alarms, and provides automated protection against evolving cyberattacks.

II. LITERATURE REVIEW

Researchers have proposed several AI-based cybersecurity systems for intrusion detection and malware analysis.

- Machine Learning algorithms such as Decision Tree, Support Vector Machine (SVM), Random Forest, and K-Nearest Neighbors (KNN) are widely used for attack classification.
- Deep Learning models such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) provide better detection of hidden attack patterns.
- Rule-based systems identify known attacks using predefined security rules.
- Hybrid AI systems combine ML and DL approaches to improve cybersecurity performance.

Although these techniques improve intrusion detection, existing systems still face limitations such as:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

1. High false positive rates.
2. Poor detection of unknown attacks.
3. Slow response time.
4. Limited scalability in large networks.
5. Difficulty adapting to evolving cyber threats.

The proposed framework addresses these challenges using integrated hybrid AI techniques.

III. OBJECTIVES OF THE PROPOSED FRAMEWORK

The major objectives of the proposed framework are:

1. To detect cyber threats at an early stage.
2. To prevent unauthorized system access.
3. To improve threat detection accuracy.
4. To minimize false positive and false negative rates.
5. To provide real-time automated cybersecurity monitoring.
6. To improve scalability and adaptability.

IV. PROPOSED HYBRID AI FRAMEWORK

A. Framework Architecture

The proposed framework combines Machine Learning, Deep Learning, and rule-based analysis to provide intelligent threat detection and prevention.

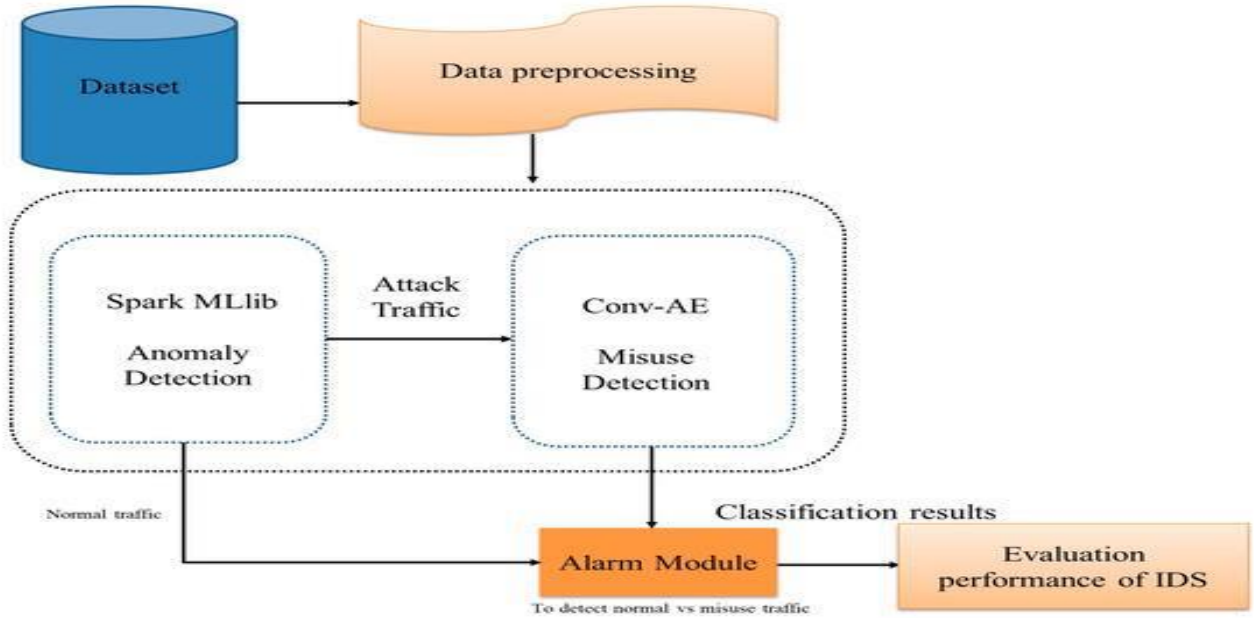

Fig. 1. Applications of the Proposed Hybrid AI-based Cybersecurity Framework

Main Components

1. Data Collection Module

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

2. Data Preprocessing Module
3. Feature Extraction Module
4. Machine Learning Detection Engine
5. Deep Learning Analysis Engine
6. Rule-Based Expert System
7. Threat Prevention Module
8. Monitoring and Alert System

B. Data Collection Module

The framework collects data from multiple cybersecurity sources such as:

- Network traffic logs :
  Network traffic logs maintain a detailed record of all data packets and communication activities occurring within a network.
- Firewall records :
  Firewall records store information about incoming and outgoing network connections that pass through a firewall security system
- User activity logs :
  User activity logs document the actions performed by users within a system, application, or network environment.
- Cloud server logs:
  Cloud server logs contain operational and security-related information generated by cloud-based platforms, virtual machines, and hosted services. These logs record events such as user authentication attempts, API requests, resource utilization, application errors, and server performance metrics.
- IoT device logs :
  IoT device logs are generated by Internet of Things devices such as smart sensors, wearable devices, industrial machines, and connected home appliances. These logs capture device status updates, communication events, sensor readings, firmware activities, and error reports.
- System event records :
  System event records maintain information about significant events occurring within an operating system or computing environment

Example Datasets

Dataset	**Purpose**
NSL-KDD	Intrusion Detection
CICIDS2017	Network Attack Analysis
UNSW-NB15	Malware Detection
Bot-IoT	IoT Threat Analysis

C. Data Preprocessing Module

Raw cybersecurity data often contains noise, duplicate entries, and missing values. Data preprocessing improves AI model performance.

Preprocessing Techniques

- Data cleaning :

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

The process of identifying and removing incorrect, duplicate, incomplete, or irrelevant data from a dataset is known as Data cleaning. It improves data quality and ensures accurate analysis and reliable results in data analytics and machine learning applications.

- Data normalisation:

  Here is the technique of scaling numerical values into a common range, usually between 0 and 1.

- Feature scaling :

  It is the process of adjusting the range of independent variables or features in a dataset.

- Handling missing values :

  It refers to the process of managing incomplete or unavailable data in a dataset.

- Encoding categorical data :

  It is the process of converting text-based or categorical information into numerical form so that machine learning algorithms can process it effectively.

Python Example

```
from sklearn.preprocessing import StandardScaler
scaler = StandardScaler()
scaled_data = scaler.fit_transform(data)
```

D. Feature Extraction Module

Feature extraction identifies important attributes from network traffic data.

Important Features

- IP address :

  An IP (Internet Protocol) address is a unique numerical identifier assigned to each device connected to a network. In cybersecurity and network analysis, IP addresses help identify the source and destination of network traffic, enabling the detection of suspicious or unauthorized activities.

- Packet size

  Packet size refers to the amount of data transmitted in a single network packet during communication between devices. Analyzing packet size helps identify abnormal traffic patterns, network congestion, and potential cyberattacks such as Distributed Denial of Service (DDoS) attacks.

- Connection duration

  Connection duration represents the total time for which a communication session remains active between two network devices. Unusually long or short connection durations may indicate malicious activities, unauthorized access, or abnormal network behavior.

- Protocol type

  Protocol type refers to the communication protocol used for data transmission over a network, such as TCP, UDP, or HTTP. Monitoring protocol types helps in understanding network behavior and detecting suspicious communication patterns associated with cyber threats.

- Login attempts :

  Login attempts indicate the number of times a user or system tries to access an account or network resource. Multiple failed login attempts may suggest brute-force attacks, unauthorized access attempts, or credential misuse.

- CPU usage patterns :

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

CPU usage patterns describe the processing activity and resource utilization of a computer system over time. Sudden spikes or abnormal CPU usage may indicate malware execution, unauthorized applications, or system-level cyberattacks.

Feature selection reduces computational complexity and improves detection efficiency.

V. MACHINE LEARNING DETECTION ENGINE

The Machine Learning Detection Engine is responsible for identifying and classifying normal and malicious network activities using intelligent learning algorithms. It analyzes network traffic patterns and detects potential cyber threats automatically. Machine learning models improve detection accuracy by learning from historical cybersecurity data

Common Algorithms

1. Decision Tree

Decision Tree is a supervised machine learning algorithm used for classification and prediction tasks. It classifies data by creating a hierarchical tree-like structure based on decision rules derived from input features. Decision Trees are highly effective for structured datasets and provide easy interpretation of classification results in cybersecurity applications.

2. Random Forest

Random Forest is an ensemble machine learning technique that combines multiple Decision Trees to improve classification accuracy and reliability. It reduces overfitting by aggregating predictions from several trees and enhances the detection of malicious network activities in cybersecurity systems

3. Support Vector Machine (SVM)

Support Vector Machine (SVM) is a supervised learning algorithm used for classification and anomaly detection. It separates normal and malicious network traffic by identifying an optimal decision boundary between different classes. SVM performs efficiently in high-dimensional datasets and is widely used in intrusion detection systems

4. K-Nearest Neighbors (KNN)

K-Nearest Neighbors (KNN) is a similarity-based machine learning algorithm that classifies data based on the nearest neighboring data points. In cybersecurity, KNN helps identify suspicious network behavior by comparing traffic patterns with previously known attack and normal activity patterns.

Python Example

```
from sklearn.ensemble import RandomForestClassifier
model = RandomForestClassifier()
model.fit(X_train, y_train)

predictions = model.predict(X_test)
```

VI. DEEP LEARNING THREAT ANALYSIS ENGINE

Deep Learning Models

A. Convolutional Neural Network (CNN)

Convolutional Neural Network (CNN) is a deep learning model widely used for identifying complex and hidden attack patterns within large cybersecurity datasets.

B. Recurrent Neural Network (RNN)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Recurrent Neural Network (RNN) is a deep learning technique designed for processing sequential and time-dependent data.

C. Long Short-Term Memory (LSTM)

Long Short-Term Memory (LSTM) is an advanced form of Recurrent Neural Network capable of learning long-term dependencies in sequential data.

Example

```
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import Dense
model = Sequential()
model.add(Dense(64, activation='relu'))
model.add(Dense(1, activation='sigmoid'))
```

VII. RULE-BASED EXPERT SYSTEM

The rule-based expert system detects known threats using predefined security rules.

Example Rules

- Multiple failed login attempts trigger alerts.
- Unusual traffic volume indicates DDoS attacks.
- Unauthorized file access generates warnings.

Advantages

- Fast detection of known threats.
- Easy interpretation of security policies.
- Supports automated response systems.

VIII. THREAT PREVENTION AND RESPONSE MODULE

The prevention module automatically responds to detected threats.

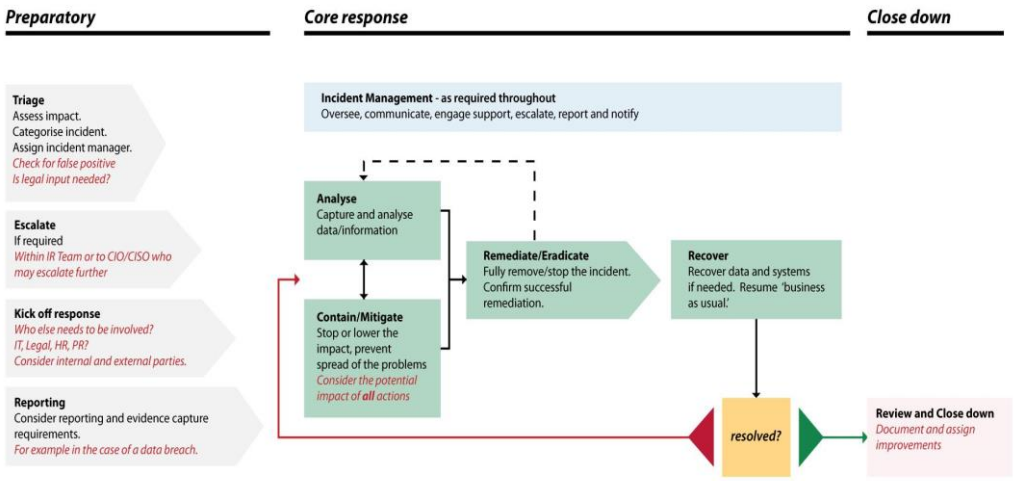

Fig. 2. Threat Prevention and Response Workflow in the Proposed Hybrid AI Framework

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Prevention Techniques

- Blocking suspicious IP addresses
- Isolating infected devices
- Updating firewall rules
- Resetting compromised sessions
- Generating security alerts

The automated response mechanism minimizes system damage and improves cybersecurity reliability.

IX. SYSTEM WORKFLOW

The workflow of the proposed framework includes:

1. Continuous collection of network data.
2. Data preprocessing and cleaning.
3. Feature extraction and selection.
4. Machine Learning classification.
5. Deep Learning behavioral analysis.
6. Rule-based validation.
7. Threat prevention and blocking.
8. Alert generation and monitoring.

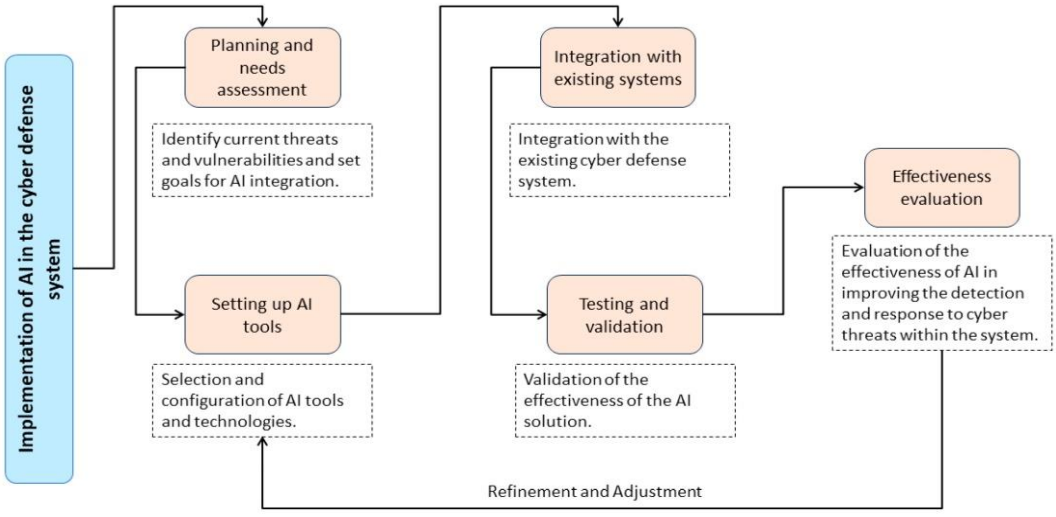

Fig. 3. Implementation Workflow of AI in Cyber Defense Systems

X. ADVANTAGES OF THE PROPOSED FRAMEWORK

The proposed hybrid AI framework provides several benefits:

1. High detection accuracy.
2. Early identification of cyber threats.
3. Reduced false positive rates.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

4. Real-time automated monitoring.
5. Improved scalability for enterprise systems

XI. APPLICATIONS OF THE FRAMEWORK

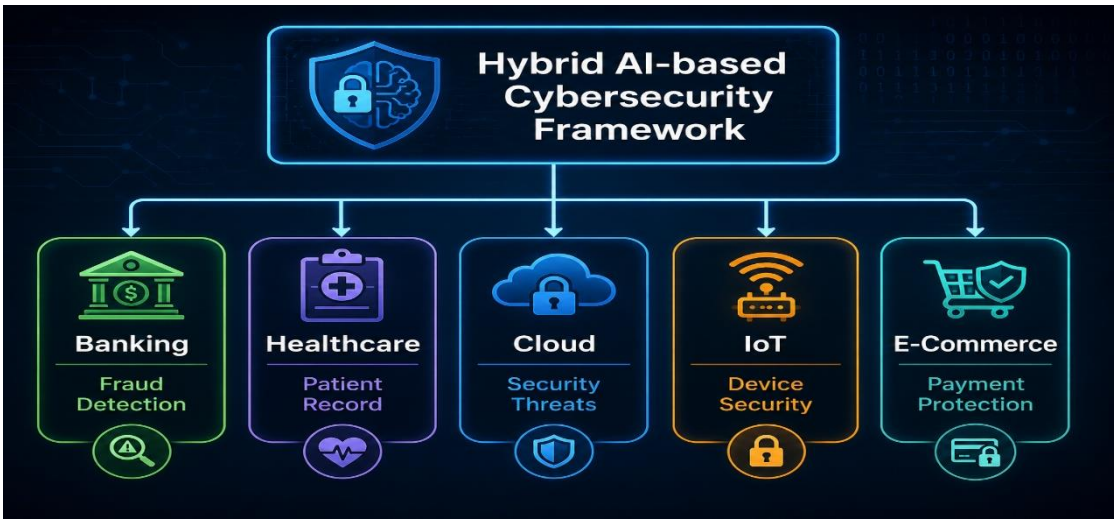

Fig. 4. Applications of the Proposed Hybrid AI-based Cybersecurity Framework

A. Banking and Finance

The proposed hybrid artificial intelligence framework plays a significant role in enhancing cybersecurity within banking and financial systems. The framework helps detect fraudulent transactions by analyzing abnormal transaction patterns and suspicious user activities in real time. Additionally, it prevents unauthorized account access through intelligent authentication monitoring and anomaly detection mechanisms.

B. Healthcare

In healthcare environments, the framework provides enhanced protection for sensitive patient records and medical information systems. The integration of AI-based cybersecurity mechanisms helps secure hospital information systems against ransomware attacks, unauthorized access, and data breaches, thereby ensuring patient data confidentiality and system reliability.

C. Cloud Computing

The framework improves security in cloud computing environments by detecting cloud-based cyberattacks and malicious activities. It continuously monitors virtualized infrastructures and protects virtual machine environments from unauthorized access, malware infections, and network intrusions through intelligent threat analysis.

D. Internet of Things (IoT)

In IoT environments, the proposed framework monitors connected smart devices and identifies abnormal communication behavior. The hybrid AI model effectively detects IoT botnet attacks and enhances the security of interconnected devices by performing continuous real-time threat monitoring and anomaly detection.

E. E-Commerce

The framework strengthens cybersecurity in e-commerce platforms by detecting phishing attacks and preventing unauthorized financial activities. It secures online payment systems through intelligent transaction analysis, fraud detection mechanisms, and real-time monitoring of suspicious user behavior.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

XII. EXPERIMENTAL ANALYSIS

The framework is evaluated using standard cybersecurity datasets.

Performance Metrics

Metric	Description
Accuracy	Measures correct predictions
Precision	Measures relevant threat detection
Recall	Measures attack detection capability
F1-Score	Balances precision and recall
Detection Time	Measures response speed

Performance Comparison

Model	Accuracy
Traditional IDS	82%
Machine Learning IDS	90%
Deep Learning IDS	94%
Proposed Hybrid AI Framework	97%

The hybrid framework demonstrates superior cybersecurity performance compared to conventional systems.

XIII. CHALLENGES AND LIMITATIONS

Despite its advantages, the framework faces several challenges:

Despite the advantages of the proposed hybrid artificial intelligence framework, several challenges and limitations remain in practical cybersecurity implementations. The framework requires high computational resources for processing large-scale network traffic and training complex machine learning models. Additionally, the performance of the system heavily depends on the availability of large and high-quality datasets for accurate threat detection.

Data privacy and security concerns also present significant challenges, particularly when handling sensitive organizational and user information. The complexity involved in training and optimizing machine learning and deep learning models increases implementation difficulty and maintenance costs. Furthermore, continuous updates and retraining are necessary to ensure that the framework remains effective against evolving cyber threats and newly emerging attack patterns.

XIV. FUTURE SCOPE

Future advancements in the proposed hybrid artificial intelligence framework may significantly enhance cybersecurity capabilities and improve adaptive threat detection mechanisms. The integration of blockchain technology can provide secure and tamper-resistant cybersecurity infrastructures for protecting sensitive organizational data. Federated learning approaches may support privacy-preserving threat analysis by enabling distributed model training without sharing confidential data across centralized systems.

Quantum AI-based threat analysis has the potential to improve computational efficiency and accelerate complex cybersecurity operations for detecting sophisticated cyberattacks. Edge AI can enhance IoT security by enabling real-time threat detection and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

decision-making closer to connected devices. Furthermore, autonomous self-learning cybersecurity systems may continuously adapt to evolving attack patterns and automatically improve defense mechanisms without extensive human intervention.

XV. CONCLUSION

Cybersecurity threats continue to evolve rapidly, making traditional security mechanisms insufficient for modern digital environments. This paper proposed a Hybrid Artificial Intelligence Framework for early detection and prevention of cyber threats. The framework combines Machine Learning, Deep Learning, and rule-based systems to improve detection accuracy and automate cybersecurity responses.

Experimental analysis demonstrates that the proposed hybrid AI model provides faster detection, higher accuracy, and reduced false positives compared to traditional intrusion detection systems. The framework can significantly improve cybersecurity protection in cloud computing, IoT networks, healthcare systems, banking infrastructures, and enterprise applications.

Future advancements in AI technologies will further strengthen intelligent cybersecurity systems and support the development of secure digital environments.

REFERENCES

[1] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2020.
[2] W. Stallings, *Network Security Essentials*, 7th ed. Pearson, 2017.
[3] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.
[4] M. Roesch, “Snort: Lightweight intrusion detection for networks,” in *Proceedings of USENIX LISA*, 1999.
[5] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” in *Military Communications and Information Systems Conference*, 2015.
[6] A. Javaid et al., “A deep learning approach for network intrusion detection system,” in *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, 2016.
[7] Cisco Annual Cybersecurity Report, Cisco Systems, 2023.
[8] IBM Security Report, IBM Corporation, 2024.
[9] Microsoft Security Intelligence Report, Microsoft Corporation, 2024.
[10] OWASP Foundation, “Top 10 Web Application Security Risks,” 2023.