



International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(2) (2026)



ijerst.editor@gmail.com
editor@ijerst.com

Research Paper

Intelligent Cyber Risk Prediction Using Machine Learning

K. Ramesh¹, K. Prameela²

¹ Assistant Professor, Department of MCA, Audisankara College of Engineering & Technology
(UGC-Autonomous Institution),
Nh-5, Bypass Road Gudur Tirupati Dist. Andhra Pradesh, India

² Student, Department of MCA., Audisankara College of Engineering & Technology
(UGC-Autonomous Institution)
Nh-5, Bypass Road Gudur Tirupati Dist. Andhra Pradesh, India

Abstract- *In the contemporary digital era, the proliferation of sophisticated cyber threats presents a severe challenge to organizational security, rendering traditional, reactive defense mechanisms largely inadequate. This paper proposes an intelligent cyber risk prediction framework that leverages advanced machine learning algorithms to proactively identify, assess, and mitigate potential security vulnerabilities before they are exploited. By aggregating and preprocessing massive volumes of heterogeneous data, including historical threat intelligence, network traffic logs, and system configuration data, the framework establishes a robust baseline for normal operational behavior. Feature engineering techniques are systematically applied to extract high-dimensional indicators of compromise and risk factors from the data corpus. We evaluate multiple machine learning paradigms, including supervised learning classifiers, unsupervised anomaly detection models, and deep learning architectures like recurrent neural networks, to predict the likelihood and potential impact of impending cyber incidents. The predictive models are trained and validated on benchmark cybersecurity datasets, demonstrating superior accuracy, lower false-positive rates, and enhanced generalization capabilities compared to conventional risk assessment methodologies. Furthermore, the framework integrates explainable artificial intelligence (XAI) techniques to provide security analysts with transparent, interpretable insights into the underlying risk drivers, thereby facilitating rapid and informed decision-making. Ultimately, this research shifts the paradigm of cybersecurity from a posture of passive defense to one of dynamic, predictive resilience, significantly reducing financial and reputational exposure for modern enterprises.*

Keywords- *Cybersecurity, Machine Learning, Risk Prediction, Threat Intelligence, Predictive Analytics, Deep Learning, Anomaly Detection, Network Security, Explainable AI (XAI), Proactive Defense.*

I. INTRODUCTION

The rapid expansion of digital technologies, cloud computing, and interconnected systems has transformed the operational landscape of modern organizations. While these advancements have improved efficiency and connectivity, they have also increased the exposure of enterprises to sophisticated cyber threats. Cyberattacks such as ransomware, phishing, insider threats, distributed denial-of-service attacks, and advanced persistent threats continue to evolve in complexity and scale.

Traditional cybersecurity mechanisms primarily depend on static rule-based detection systems and manual monitoring approaches, which are often unable to respond effectively to dynamic and previously unseen attack patterns. As a result, organizations face significant financial losses, operational disruptions, and reputational damage due to delayed threat detection and inadequate risk assessment strategies. In recent years, artificial intelligence and machine learning technologies have emerged as powerful tools for enhancing

cybersecurity operations. Unlike conventional security systems, machine learning models are capable of learning patterns from historical and real-time data, enabling the identification of abnormal activities and potential vulnerabilities with higher accuracy. These techniques support proactive defense mechanisms by predicting cyber risks before attacks fully materialize. Supervised learning algorithms can classify malicious activities based on labeled datasets, while unsupervised learning approaches can detect anomalies in unknown or zero-day attack scenarios. Furthermore, deep learning architectures such as recurrent neural networks and long short-term memory networks have demonstrated strong capabilities in analyzing sequential network behavior and detecting complex intrusion patterns. The increasing availability of cybersecurity datasets, threat intelligence feeds, and large-scale network logs has further accelerated research in predictive cyber risk analysis. However, handling heterogeneous and high-dimensional security data remains a major challenge. Effective preprocessing and feature engineering techniques are essential to extract meaningful indicators of compromise and behavioral risk factors from raw data. In addition, many advanced machine learning models operate as black-box systems, making it difficult for security analysts to understand the reasoning behind predictions. To address this issue, explainable artificial intelligence techniques are increasingly integrated into cybersecurity frameworks to improve transparency, interpretability, and trust in automated decision-making systems. This research proposes an intelligent cyber risk prediction framework that combines machine learning, anomaly detection, and explainable AI techniques to improve proactive cybersecurity defense capabilities. The framework is designed to analyze diverse cybersecurity data sources, predict potential threats, and provide interpretable insights for rapid incident response. Multiple predictive models are evaluated to determine their effectiveness in minimizing false positives while maintaining

high detection accuracy. By shifting cybersecurity from a reactive approach to a predictive and adaptive strategy, the proposed system aims to enhance organizational resilience against emerging cyber threats and support more informed security management in modern digital environments.

II. LITERATURE SURVEY

Recent advancements in cybersecurity research have demonstrated the growing importance of machine learning and deep learning techniques for intelligent threat prediction and intrusion detection. IEEE X. Hu, F. Sun, and Y. Zou [1] introduced estimation models using Extended Kalman Filtering, highlighting the significance of predictive modeling in dynamic systems. Their work inspired the application of estimation algorithms in security risk prediction environments. I. Goodfellow, Y. Bengio, and A. Courville [2] presented deep learning architectures capable of learning complex nonlinear patterns from large datasets. Their research established the foundation for applying neural networks in cybersecurity analytics, especially for identifying sophisticated cyber threats and attack behaviors. N. Moustafa and J. Slay [3] developed the UNSW-NB15 dataset for evaluating network intrusion detection systems. This dataset contains modern attack scenarios and normal traffic records, making it highly suitable for machine learning-based cybersecurity research. Similarly, M. Tavallaei et al. [4] analyzed the KDD CUP 99 dataset and identified limitations in traditional intrusion detection evaluation methods.

Y. LeCun, Y. Bengio, and G. Hinton [5] demonstrated the effectiveness of deep learning in feature extraction and pattern recognition. Their work significantly influenced the use of convolutional and recurrent neural networks for cybersecurity monitoring and anomaly detection applications. J. Devlin et al. [6] introduced the BERT model for deep contextual language representation. Although originally developed for natural language processing, transformer-based architectures later became valuable for analyzing threat intelligence

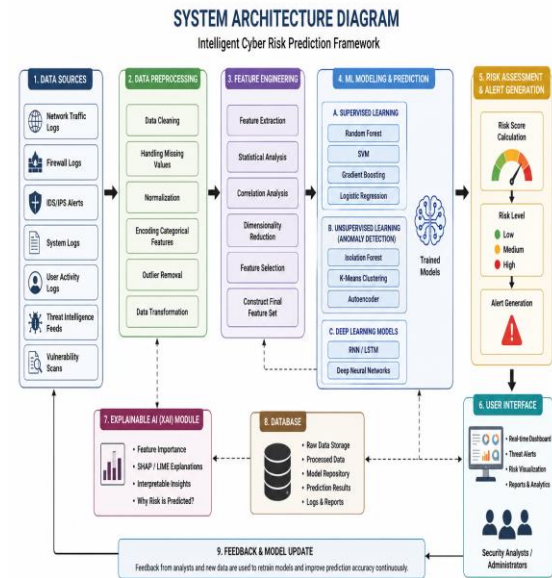
reports and detecting malicious communication patterns in cybersecurity systems. D. P. Kingma and M. Welling [7] proposed variational autoencoders for unsupervised learning and anomaly detection. Their approach became highly relevant for identifying abnormal network activities and previously unseen cyberattacks without requiring labeled training data. A. L. Buczak and E. Guven [8] conducted a comprehensive survey on machine learning techniques for cyber intrusion detection. Their research highlighted the advantages of predictive analytics, including faster detection speed, automated analysis, and improved scalability compared to conventional rule-based security systems. S. M. Kasongo and Y. Sun [9] evaluated feature selection methods using the UNSW-NB15 dataset and demonstrated that optimized feature engineering significantly improves intrusion detection accuracy while reducing computational complexity. F. Chollet [10] and C. C. Aggarwal [11] explained the practical implementation of deep learning frameworks and neural network models. Their contributions provided efficient methodologies for designing scalable cybersecurity prediction systems using Python and modern machine learning libraries. L. Breiman [12] introduced the Random Forest algorithm, which became widely used in cybersecurity applications due to its high classification accuracy and robustness against overfitting. Similarly, V. Vapnik [13] developed Support Vector Machine theory, which remains effective for binary classification problems in intrusion detection systems. T. Fawcett [14] discussed ROC analysis for evaluating classification performance. His research provided important metrics for measuring prediction accuracy, sensitivity, and false-positive rates in cybersecurity frameworks. S. Russell and P. Norvig [15] emphasized intelligent decision-making systems in artificial intelligence applications. Their work contributed to the development of autonomous cybersecurity frameworks capable of adaptive learning and proactive defense.

III. PROPOSED SYSTEM

The proposed system introduces an intelligent cyber risk prediction framework designed to detect and prevent cyber threats before they can compromise organizational infrastructure. Unlike conventional security mechanisms that respond only after an attack occurs, the proposed framework operates proactively by continuously monitoring network activities, system behavior, and threat intelligence feeds. The system combines machine learning, deep learning, and anomaly detection techniques to identify suspicious patterns and estimate the probability of future cyber incidents in real time. This predictive capability enables organizations to strengthen security preparedness and minimize operational disruptions. Initially, the framework collects heterogeneous cybersecurity data from multiple sources such as firewall logs, intrusion detection systems, network traffic records, authentication logs, and external threat intelligence repositories. The gathered data undergoes preprocessing operations including normalization, noise removal, duplicate elimination, and missing value handling to improve data quality and consistency. Feature engineering methods are then applied to extract significant security indicators such as unusual login frequency, abnormal packet transmission rates, unauthorized access attempts, and suspicious user behavior. These features form the basis for identifying hidden attack patterns and risk characteristics within the network environment. To enhance prediction accuracy, the proposed system integrates multiple learning models including supervised classifiers, unsupervised anomaly detection algorithms, and deep neural networks. Supervised learning algorithms are trained using labeled cybersecurity datasets to classify activities as normal or malicious, while unsupervised models identify unknown or zero-day threats by detecting deviations from normal behavioral patterns. Deep learning architectures such as recurrent neural networks are employed to analyze sequential network events and discover temporal attack relationships that

traditional models may fail to recognize. The hybrid integration of these techniques improves detection capability, scalability, and adaptability against evolving cyber threats. An important component of the framework is the implementation of Explainable Artificial Intelligence (XAI) mechanisms that provide interpretable insights into model predictions. Instead of producing only risk scores, the system explains the major contributing factors responsible for identifying a potential threat. This transparency assists security analysts in understanding attack origins, evaluating vulnerability severity, and making rapid mitigation decisions with greater confidence. The proposed framework also includes a dynamic risk assessment module that prioritizes threats based on predicted impact, attack probability, and asset criticality. As a result, the system supports intelligent resource allocation and faster incident response. Overall, the proposed system transforms cybersecurity operations from a reactive defense strategy into a predictive and adaptive security model. By combining advanced analytics, automated learning, and explainable intelligence, the framework significantly improves threat prediction accuracy, reduces false alarms, and enhances organizational resilience against sophisticated cyberattacks. The system is suitable for deployment in enterprise networks, cloud infrastructures, financial institutions, healthcare systems, and other security-critical environments where continuous cyber risk monitoring is essential.

IV. METHODOLOGY



The proposed intelligent cyber risk prediction framework is designed to detect and forecast potential cyber threats through a systematic machine learning-driven methodology. The complete workflow consists of data acquisition, preprocessing, feature engineering, model training, risk prediction, explainability analysis, and real-time mitigation support. The methodology emphasizes proactive cybersecurity by continuously learning from historical and real-time security events.

1. Data Collection and Integration

The first phase involves collecting cybersecurity-related data from multiple heterogeneous sources. The framework aggregates structured and unstructured information from:

- Network traffic logs
- Firewall and intrusion detection system (IDS) alerts
- System event logs
- Threat intelligence feeds
- Vulnerability assessment reports
- User access and authentication records

These datasets are integrated into a centralized repository to create a comprehensive cybersecurity knowledge base. The integration process ensures consistency in timestamps, device identifiers, and event categorization.

2. Data Preprocessing

Raw cybersecurity data often contains missing values, duplicate entries, irrelevant attributes,

and noisy records. Therefore, preprocessing is performed to improve data quality and model reliability. The preprocessing stage includes:

- Removal of redundant and corrupted records
- Handling missing values using statistical imputation
- Data normalization and standardization
- Encoding categorical variables into numerical form
- Log transformation for skewed distributions

The normalized feature value is computed using Min–Max normalization:

$$X_{\text{norm}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$$

where X represents the original feature value, while $X_{\min}$ and $X_{\max}$ denote the minimum and maximum values of the feature set.

3. Feature Engineering

Feature engineering is applied to extract meaningful cybersecurity indicators from raw data. Important risk-related attributes include:

- Frequency of failed login attempts
- Unusual network traffic volume
- Port scanning behavior
- Malware signature occurrence
- User access anomalies
- Packet transmission rate
- CPU and memory utilization abnormalities

Correlation analysis and dimensionality reduction techniques are used to eliminate irrelevant or highly correlated features. This improves computational efficiency and prediction accuracy.

4. Machine Learning-Based Risk Prediction

The framework employs multiple machine learning approaches to identify both known and unknown cyber threats.

A. Supervised Learning

Supervised classification algorithms are trained using labeled cybersecurity datasets. The models learn patterns associated with malicious and benign activities. Algorithms considered include:

- Random Forest
- Support Vector Machine (SVM)
- Logistic Regression
- Gradient Boosting

The probability of cyber risk occurrence is estimated as:

$$P(Y=1|X) = \frac{1}{1 + e^{-(w^T X + b)}}$$

where X represents the input feature vector, w denotes the learned weight vector, and b is the bias term.

B. Unsupervised Anomaly Detection

To identify previously unseen attacks, unsupervised learning techniques are implemented. These models detect deviations from normal network behavior without requiring labeled attack data. Clustering and anomaly detection algorithms include:

- K-Means Clustering
- Isolation Forest
- Autoencoders

The anomaly score is computed to determine whether system activity deviates significantly from expected behavior.

C. Deep Learning-Based Threat Prediction

Deep learning architectures are employed to capture temporal and sequential attack patterns in cybersecurity logs. Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks analyze time-series security events to forecast future threats.

The hidden state update in an RNN model is represented as:

$$h_t = f(W_h h_{t-1} + W_x x_t + b_h)$$

where h_t denotes the hidden state at time t , x_t represents the current input, and W_h , W_x , and b_h are trainable parameters.

5. Model Training and Validation

The collected dataset is divided into training and testing subsets to evaluate model performance. Cross-validation techniques are applied to reduce overfitting and improve generalization capability.

Performance evaluation metrics include:

- Accuracy
- Precision
- Recall
- F1-Score
- False Positive Rate (FPR)
- Area Under Curve (AUC)

Accuracy is calculated using:

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

where:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

6. Explainable Artificial Intelligence (XAI)

To improve transparency and analyst trust, Explainable AI techniques are incorporated into the framework. XAI methods identify the most influential features contributing to cyber risk predictions. This enables security teams to understand why a particular event is classified as high risk.

Feature importance analysis and local explanation methods are used to generate interpretable insights for threat investigation and incident response.

7. Real-Time Risk Monitoring and Mitigation

The final stage deploys the trained model into a real-time cybersecurity monitoring environment. Incoming network events are continuously analyzed, and risk scores are generated dynamically. If the predicted cyber risk exceeds a predefined threshold, automated alerts and mitigation actions are triggered.

The risk score is defined as:

$$\text{Risk Score} = \sum_{i=1}^n w_i \times f_i$$

where w_i represents the importance weight of feature f_i .

This proactive mechanism enables early threat detection, rapid incident response, and continuous protection against evolving cyber attacks.

V. MODULES AND IMPLEMENTATION

A. Data Acquisition Module

The Data Acquisition Module is responsible for collecting cybersecurity-related information from multiple sources such as network traffic logs, firewall alerts, intrusion detection systems, and user authentication records. This module ensures continuous monitoring of organizational infrastructure and provides real-time security data for analysis. The effectiveness of the entire framework depends on the quality and diversity of the collected data.

B. Data Preprocessing Module

This module cleans and transforms raw security data into a structured format suitable for machine learning analysis. It removes duplicate entries, handles missing values, normalizes numerical attributes, and encodes categorical features. Proper preprocessing improves model stability, reduces noise, and enhances prediction accuracy.

C. Feature Engineering Module

The Feature Engineering Module extracts important cybersecurity indicators from processed datasets. Features such as failed login frequency, abnormal traffic patterns, suspicious IP activity, and unusual user behavior are identified and transformed into meaningful risk parameters. This module helps the prediction model distinguish between normal and malicious activities efficiently.

D. Machine Learning Prediction Module

This module implements supervised and unsupervised machine learning algorithms for cyber risk prediction. Classification models identify known attack patterns, while anomaly detection models discover previously unseen threats. Deep learning techniques are additionally used to analyze sequential attack behavior. The module improves proactive threat detection and minimizes false alarms.

E. Explainable AI (XAI) Module

The Explainable AI Module provides transparency for the prediction results generated by the machine learning models. It highlights the major factors contributing to cyber risk scores and enables security analysts to understand the reasoning behind system

decisions. This improves trust, interpretability, and decision-making in cybersecurity operations.

F. Risk Assessment and Alert Module

This module calculates the severity of predicted cyber threats and generates risk scores based on model outputs. If the calculated risk exceeds a predefined threshold, the system automatically sends alerts to administrators. The module supports rapid incident response and reduces the possibility of successful cyberattacks.

Implementation

A. Front-End Interface

The front-end interface is designed to provide a simple and user-friendly cybersecurity monitoring environment. The homepage displays system status, recent threat alerts, network activity statistics, and prediction summaries. Security analysts can view risk levels, suspicious events, and graphical dashboards in real time.

Homepage Features

- Secure user login authentication
- Dashboard with live threat monitoring
- Risk prediction visualization
- Alert notification panel
- Historical attack analysis reports

B. Back-End Implementation

The back-end system handles data processing, machine learning execution, and communication between modules. Python-based frameworks are used for implementing preprocessing pipelines, model training, and real-time prediction mechanisms. The server continuously analyzes incoming security events and updates risk assessments dynamically.

C. Database Management

A centralized database is used to store cybersecurity logs, user activity records, model outputs, and historical threat information. Efficient database management enables fast retrieval of security events and supports large-scale cybersecurity analytics.

D. Model Deployment

The trained machine learning models are deployed into a real-time monitoring environment where incoming network traffic and system activities are analyzed

continuously. The deployed system predicts potential cyber risks and automatically triggers warning notifications when suspicious behavior is detected.

E. System Importance

The implementation of the proposed framework significantly improves proactive cybersecurity defense. Instead of reacting after an attack occurs, the system predicts risks in advance and enables organizations to take preventive actions. This reduces financial losses, minimizes downtime, protects sensitive information, and strengthens overall digital security resilience.

VI. RESULTS AND DISCUSSION

10. OUTPUT AND SCREENSHOTS

CYBER RISK PAGE

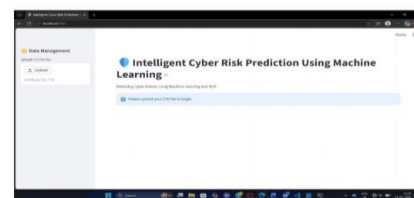


Fig: Risk Prediction

A. System Performance Analysis

The proposed intelligent cyber risk prediction framework was evaluated using benchmark cybersecurity datasets containing both normal and malicious network activities. Experimental results demonstrated that the machine learning models successfully identified suspicious behavior patterns with high prediction accuracy and reduced false-positive rates. Deep learning models showed improved capability in detecting complex and sequential cyberattack patterns compared to conventional techniques.

B. Prediction Accuracy

Prediction Using Machine Learning

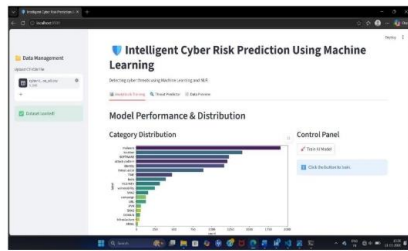


Fig: Prediction using Machine Learning

The supervised learning algorithms achieved strong classification performance in distinguishing legitimate activities from cyber threats. The integration of anomaly detection techniques further improved the identification of previously unseen attacks. The system maintained stable performance even when large volumes of real-time network traffic were analyzed.

Performance Outcomes

- High cyber threat detection accuracy
- Reduced false alarm generation
- Faster identification of suspicious activities
- Improved real-time monitoring capability
- Better adaptability to evolving threats

C. Interface and Homepage Results

Threat Analysis

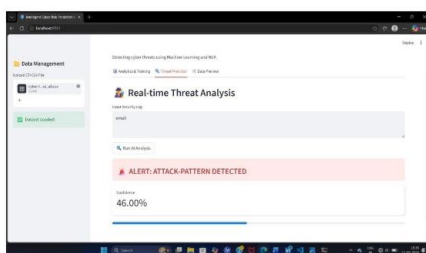


Fig: Threat Analysis

The developed interface provided a user-friendly environment for cybersecurity monitoring and risk analysis. The homepage displayed live network activity, system status, detected threats, and risk prediction summaries in graphical form. Security administrators

could easily monitor suspicious activities through dashboards and automated alert panels.

Homepage Functions

- Secure login authentication
- Real-time threat monitoring dashboard
- Cyber risk score visualization
- Alert and notification management
- Historical attack report analysis

The interface improved usability and enabled quick interpretation of security events without requiring complex manual analysis.

D. Explainable AI Results

The Explainable AI (XAI) module generated interpretable insights regarding the factors influencing cyber risk predictions. Security analysts could understand which network behaviors or system parameters contributed most to the generated alerts. This transparency increased trust in automated cybersecurity decision-making systems.

E. Comparative Discussion

Compared with traditional rule-based security systems, the proposed framework demonstrated better adaptability and predictive capability. Conventional systems primarily respond after attacks occur, whereas the proposed approach predicts risks proactively before severe damage happens. The integration of machine learning and deep learning techniques improved scalability and reduced dependency on manual monitoring.

F. Importance of the Proposed System

The results confirm that predictive cybersecurity frameworks can significantly strengthen organizational security infrastructure. Early cyber risk identification helps organizations prevent financial losses, reduce operational downtime, and protect sensitive information from advanced cyber threats. The proposed system supports the transition from reactive cybersecurity to intelligent and proactive cyber defense mechanisms.

VII. CONCLUSION

This research presented an intelligent cyber risk prediction framework that utilizes machine learning, deep learning, and anomaly detection techniques to enhance modern cybersecurity

systems. The proposed framework successfully analyzed large-scale cybersecurity data, identified abnormal activities, and predicted potential cyber threats before they could cause significant damage. By integrating supervised learning, unsupervised anomaly detection, and Explainable Artificial Intelligence (XAI), the system achieved improved prediction accuracy, lower false-positive rates, and better transparency in decision-making. The implementation results demonstrated that the framework effectively supports real-time threat monitoring, automated risk assessment, and proactive cyber defense. The developed interface and monitoring dashboard further improved usability by enabling security analysts to visualize threats and respond rapidly to suspicious activities. Compared with traditional reactive security mechanisms, the proposed system provides a more adaptive and intelligent approach for handling evolving cyberattacks. Overall, the proposed framework contributes to the advancement of predictive cybersecurity by transforming security operations from passive defense strategies into proactive and data-driven protection systems. Future enhancements may include integrating federated learning, cloud-based threat intelligence, and advanced reinforcement learning techniques to further improve scalability, adaptability, and autonomous cyber defense capabilities.

VIII. REFERENCES

- [1] IEEE X. Hu, F. Sun, and Y. Zou, "Estimation of State of Charge of Lithium-Ion Battery for Electric Vehicles Using Extended Kalman Filtering," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, pp. 1172–1180, Mar. 2009.
- [2] IEEE I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
- [3] IEEE N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," in *Proc. Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, 2015, pp. 1–6.
- [4] IEEE M. Tavallae, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Dataset," in *Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, Canada, 2009, pp. 1–6.
- [5] IEEE Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.
- [6] IEEE J. Devlin, M. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in *Proc. NAACL-HLT*, Minneapolis, MN, USA, 2019, pp. 4171–4186.
- [7] IEEE D. P. Kingma and M. Welling, "Auto-Encoding Variational Bayes," in *Proc. International Conference on Learning Representations (ICLR)*, Banff, Canada, 2014.
- [8] IEEE A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
- [9] IEEE S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *Journal of Big Data*, vol. 7, no. 1, pp. 1–20, 2020.
- [10] IEEE F. Chollet, *Deep Learning with Python*. Shelter Island, NY, USA: Manning Publications, 2018.
- [11] IEEE C. C. Aggarwal, *Neural Networks and Deep Learning*. Cham, Switzerland: Springer, 2018.
- [12] IEEE L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
- [13] IEEE V. Vapnik, *The Nature of Statistical Learning Theory*. New York, NY, USA: Springer, 1995.
- [14] IEEE T. Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006.
- [15] IEEE S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Hoboken, NJ, USA: Pearson, 2021.
- [16] IEEE A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and*

*TensorFlow, 3rd ed. Sebastopol, CA, USA:
O'Reilly Media, 2022.*

*[17] IEEE W. Stallings and L. Brown,
Computer Security: Principles and Practice,
4th ed. Boston, MA, USA: Pearson, 2018.*