International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Attack Prediction from Traditional ML to Generative Artificial Intelligence

Jaswanth Syam Sundar Garugu

M.Tech Graduate, Computer Science and Engineering. Independent Researcher

Abstract

The increasing frequency and sophistication of cyber attacks have created a growing demand for intelligent and proactive intrusion detection systems capable of accurately identifying evolving network threats. This paper presents an AI-driven cyber attack prediction framework that integrates machine learning, deep learning, generative artificial intelligence, and explainable artificial intelligence techniques using the CICIDS2017 dataset. The dataset is preprocessed through data cleaning, feature transformation, normalization, and principal component analysis to improve data quality and computational efficiency. Multiple machine learning and deep learning models are comparatively evaluated, while generative AI models are employed to simulate synthetic attack patterns and enhance anomaly representation. Experimental results demonstrate that the ensemble Voting Classifier achieves the highest classification accuracy of 99.6%, whereas the LSTM model attains 99.3%, indicating the effectiveness of ensemble learning and sequential deep learning for cyber attack prediction. Model interpretability is enhanced using LIME and SHAP, enabling transparent explanation of prediction outcomes. Furthermore, a Flask-based deployment framework facilitates real-time network traffic classification and visualization, providing an interpretable and scalable solution for intelligent cybersecurity applications.

Keywords: Cyber attack prediction, Intrusion detection, Machine learning, Deep learning, Generative artificial intelligence, Explainable artificial intelligence, Ensemble learning, Network security".

INTRODUCTION

The rapid growth of digital technologies and the widespread adoption of cloud computing, Internet of Things (IoT), and interconnected communication networks have significantly increased the complexity of modern cyber threats. Organizations across healthcare, finance, government, and industrial sectors continuously exchange sensitive information over networked environments, making them attractive targets for cyberattacks. Threats such as distributed denial-of-service (DDoS) attacks, ransomware, phishing, botnets, and data breaches have become increasingly sophisticated, causing financial losses, operational disruptions, and unauthorized access to critical information. Consequently, developing intelligent cybersecurity systems capable of accurately detecting and predicting cyber threats has become an important research challenge [1], [2].

Artificial Intelligence (AI) has emerged as a promising solution for enhancing cybersecurity by enabling automated threat detection and predictive analysis. Machine Learning (ML) techniques can identify malicious traffic patterns from historical network data, while Deep Learning (DL) models are capable of learning complex spatial and temporal relationships that improve intrusion detection performance. Recent

studies have demonstrated that AI-driven approaches significantly outperform conventional signature-based security mechanisms when identifying previously unseen attacks [3], [7].

Despite these advancements, several challenges remain. Many existing intrusion detection systems rely on a single learning paradigm, resulting in limited generalization capability and reduced adaptability against evolving attack patterns. Furthermore, the lack of model interpretability makes security analysts hesitant to rely entirely on automated predictions. In addition, practical deployment of AI models requires efficient preprocessing, scalable inference, and seamless integration with real-world cybersecurity environments [6], [13].

To address these limitations, this paper presents an AI-driven cyberattack prediction framework that integrates conventional Machine Learning, Deep Learning, Generative Artificial Intelligence, and Explainable Artificial Intelligence techniques using the CICIDS2017 benchmark dataset. The proposed framework incorporates data preprocessing, feature transformation, dimensionality reduction, comparative evaluation of multiple learning models, synthetic attack pattern generation, and interpretable prediction to improve cyberattack detection performance. A Flask-based deployment framework further enables real-time network traffic classification and visualization, providing a practical and scalable solution for intelligent cybersecurity applications.

RELATED WORK

Artificial Intelligence (AI) has significantly transformed cybersecurity by enabling intelligent threat detection, attack prediction, and automated decision-making. Early studies primarily focused on replacing conventional signature-based intrusion detection systems with data-driven learning models capable of identifying both known and previously unseen attacks. Li [3] highlighted the growing role of AI in cybersecurity, emphasizing its ability to improve network monitoring, anomaly detection, and incident response. Similarly, Sarker et al. [4] presented cybersecurity data science as an emerging discipline that combines machine learning with large-scale network analytics to strengthen predictive security mechanisms. Further advancements discussed by Sarker et al. [5] demonstrated that AI-driven cybersecurity frameworks can effectively support threat intelligence, risk assessment, and adaptive defense strategies, making them suitable for modern network environments. However, these studies also pointed out challenges related to data quality, model scalability, and deployment in dynamic infrastructures.

Deep Learning (DL) has further enhanced intrusion detection by learning complex spatial and temporal characteristics from network traffic. Ferrag et al. [7] provided a comprehensive survey of deep learning approaches for intrusion detection and reported that CNN- and LSTM-based models consistently outperform many traditional machine learning algorithms when trained on benchmark datasets. Vinayakumar et al. [8] demonstrated the effectiveness of deep neural networks in detecting sophisticated cyberattacks through automated feature learning, thereby reducing dependence on handcrafted features. Apruzzese et al. [9] compared conventional machine learning and deep learning techniques and concluded that no single model performs optimally across all attack categories, highlighting the importance of comparative evaluation. Likewise, Kwon et al. [10] emphasized that hybrid deep learning architectures are particularly effective in capturing complex traffic behaviors and temporal dependencies in large-scale network environments. Although these approaches have achieved promising detection accuracy, they often require extensive computational resources and lack sufficient interpretability for practical deployment.

To improve transparency in AI-driven cybersecurity, Explainable Artificial Intelligence (XAI) has emerged as an active research area. Lundberg and Lee [12] introduced the SHAP framework, which provides

consistent feature attribution for interpreting model predictions. Zhang et al. [13] demonstrated that explainable models improve analysts' confidence by revealing the factors contributing to cyberattack predictions, while Arreche et al. [14] evaluated explainability frameworks for intrusion detection and highlighted their importance in operational security environments. More recently, Generative Artificial Intelligence has gained attention for cybersecurity applications. Gupta et al. [15] discussed the potential of large language models in threat intelligence and security automation, whereas Sai et al. [16] explored the use of generative models for attack simulation, security analysis, and defensive applications. These studies indicate that combining explainability with generative capabilities can significantly enhance the effectiveness of intelligent cybersecurity systems.

Despite substantial progress, existing studies generally investigate Machine Learning, Deep Learning, Explainable AI, or Generative AI as independent research directions. Limited attention has been given to developing an integrated framework that combines these complementary technologies while supporting comparative model evaluation and real-time deployment. Motivated by this research gap, the proposed work presents a unified AI-based cyberattack prediction framework that incorporates multiple learning paradigms, explainable prediction, generative intelligence, and a practical deployment environment to provide accurate, interpretable, and scalable cybersecurity solutions.

Materials And Methods

A. Overall Framework

The proposed framework presents an end-to-end Artificial Intelligence-based cybersecurity system for predicting cyberattacks through the integration of Machine Learning (ML), Deep Learning (DL), Generative Artificial Intelligence (GenAI), and Explainable Artificial Intelligence (XAI). The workflow begins with the acquisition of the CICIDS2017 dataset, followed by data preprocessing and feature engineering to improve data quality and model performance. Multiple ML and DL models are trained and comparatively evaluated to identify the most effective prediction model. The framework further incorporates Generative AI for intelligent threat analysis and Explainable AI techniques to improve prediction transparency. Finally, the trained framework is deployed through a Flask-based web application for real-time cyberattack prediction and visualization.

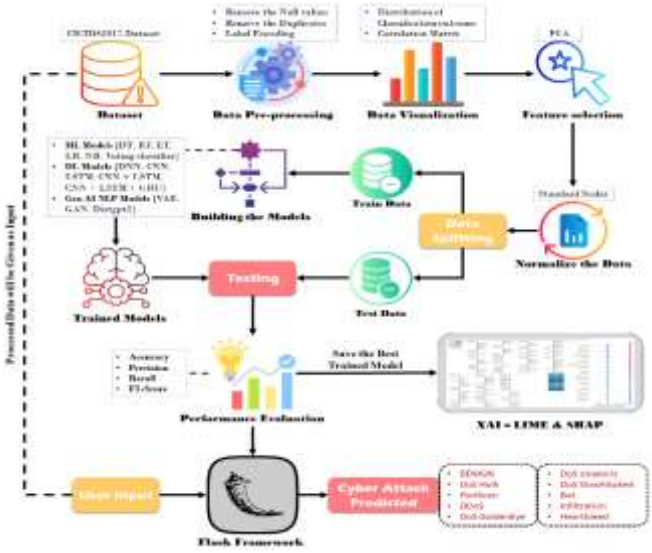
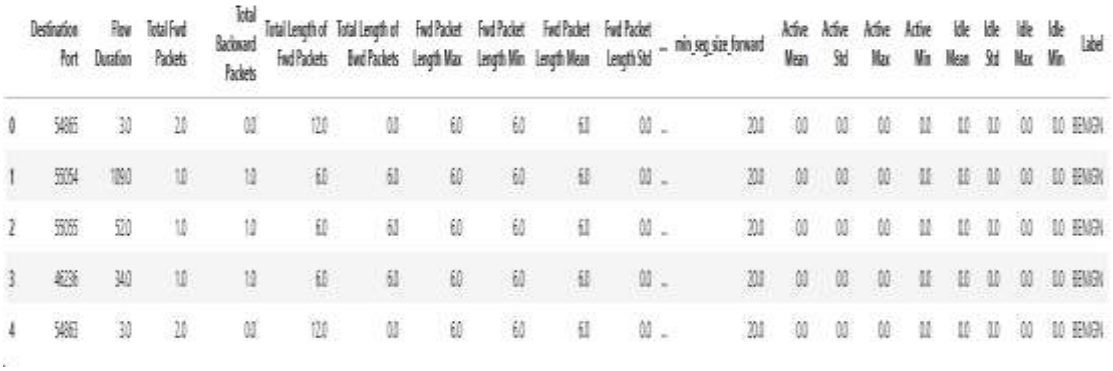


Fig. 1. System Architecture

Fig. 1 illustrates the overall architecture of the proposed cyberattack prediction framework. It depicts the complete processing pipeline, including dataset acquisition, preprocessing and feature engineering, model training and evaluation using ML and DL algorithms, Generative AI-assisted threat analysis, Explainable AI-based interpretation, and deployment through a Flask web application for real-time cyberattack prediction and visualization.

B. Dataset Description

The proposed framework utilizes the CICIDS2017 dataset, a widely adopted benchmark for evaluating intrusion detection and cyberattack prediction models. Developed by the Canadian Institute for Cybersecurity, the dataset captures realistic network traffic generated under both normal user behavior and diverse cyberattack scenarios. It includes multiple attack categories, such as Distributed Denial-of-Service (DDoS), Brute Force, Botnet, Web Attacks, PortScan, Heartbleed, and Infiltration, along with benign network traffic. Each network flow is represented by a comprehensive set of statistical and behavioral features that describe packet characteristics and communication patterns. The diversity, realism, and balanced representation of attack types make CICIDS2017 an appropriate benchmark for training, validating, and comparing AI-based cybersecurity models, thereby enabling robust and reliable cyberattack prediction [11].



	Destination Port	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total Length of Bwd Packets	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	Fwd Packet Length Std	...	min_seg_size_forward	Active Mean	Active Std	Active Max	Active Min	Idle Mean	Idle Std	Idle Max	Idle Min	Label
0	54865	3.0	2.0	0.0	12.0	0.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN
1	55054	109.0	1.0	1.0	6.0	6.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN
2	55055	52.0	1.0	1.0	6.0	6.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN
3	46236	34.0	1.0	1.0	6.0	6.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN
4	54863	3.0	2.0	0.0	12.0	0.0	6.0	6.0	6.0	0.0	...	20.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	BENIGN

Fig.2 Dataset Collection

C. Data Preprocessing and Feature Engineering

The CICIDS2017 dataset undergoes preprocessing to improve data quality and learning performance. Missing values, duplicate records, and inconsistent entries are removed before transforming categorical labels into numerical values using label encoding. Numerical features are standardized using Z-score normalization to eliminate scale variations among attributes. Subsequently, Principal Component Analysis (PCA) is applied to reduce feature dimensionality while preserving the most informative characteristics. Finally, the processed dataset is partitioned into training and testing sets for model development and evaluation.

The Z-score normalization is computed as

$$z = \frac{x - \mu}{\sigma} \qquad (1)$$

where x is the original feature value, μ is the feature mean, and σ is the standard deviation. This normalization scales all features to a common distribution, improving model convergence.

The PCA transformation is expressed as

$$Y = XW \qquad (2)$$

where X denotes the standardized feature matrix, W represents the selected principal component vectors, and Y is the transformed feature matrix. PCA reduces redundant information and computational complexity while retaining the dominant data variance.

D. Machine Learning and Deep Learning Models

The proposed framework employs multiple Machine Learning (ML) and Deep Learning (DL) algorithms to comparatively evaluate cyberattack prediction performance. The ML models include Logistic Regression, Decision Tree, Random Forest, XGBoost, LightGBM, and a Voting Classifier, whereas the DL models comprise Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and a hybrid CNN-LSTM architecture. Each model is trained using the preprocessed dataset and evaluated using standard performance metrics. The comparative analysis enables the identification of the most effective model for accurate and reliable cyberattack prediction.

The Logistic Regression model estimates the probability of an attack using the sigmoid function

$$P(y = 1 \mid x) = \frac{1}{1 + e^{-z}} \qquad (3)$$

where $z = w^T x + b$, w denotes the weight vector, x represents the input features, and b is the bias term. For deep learning, the LSTM updates its memory cell according to

$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t \qquad (4)$$

where f_t, i_t, and $\tilde{C}_t$ denote the forget gate, input gate, and candidate cell state, respectively. This memory mechanism enables the model to preserve long-term dependencies in sequential network traffic, improving the detection of sophisticated cyberattacks.

E. Generative AI and Explainable AI Integration

To further enhance cybersecurity intelligence, the proposed framework integrates Generative Artificial Intelligence (GenAI) and Explainable Artificial Intelligence (XAI). GenAI models, including ChatGPT, Gemini, Claude, DeepSeek, and Grok, are utilized to assist in threat interpretation, security report generation, attack analysis, and defensive recommendations based on prediction outcomes. In addition, XAI techniques such as SHAP and LIME improve the transparency of AI predictions by identifying influential features and providing interpretable explanations for individual cyberattack classifications. This integration enables security analysts to better understand model decisions, supports informed incident response, and increases confidence in deploying AI-driven cybersecurity solutions in practical environments.

The SHAP value for feature contribution is computed as

$$\phi_i = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(|N| - |S| - 1)!}{|N|!} [f(S \cup \{i\}) - f(S)] \qquad (5)$$

where ϕ_i represents the contribution of feature i, S denotes a subset of features, and $f(\cdot)$ is the prediction function. SHAP quantifies the impact of each feature on the prediction, thereby improving the interpretability and trustworthiness of the proposed cyberattack prediction framework.

F. Deployment Framework

To demonstrate the practical applicability of the proposed framework, the trained AI models are deployed using a Flask-based web application that supports real-time cyberattack prediction. The deployment framework provides an interactive interface for uploading network traffic data, performing automated preprocessing, and generating attack predictions using the selected ML or DL model. The prediction results are further enhanced through Generative AI-based threat interpretation and XAI-based feature explanations, enabling users to understand the rationale behind each prediction. The framework also

presents prediction outcomes and analytical insights through intuitive visualizations, thereby providing an efficient and user-friendly platform for intelligent cybersecurity monitoring and decision support.

EXPERIMENTAL RESULTS

A. Experimental Setup

The proposed cyberattack prediction framework was evaluated using the CICIDS2017 benchmark dataset, which contains realistic benign and malicious network traffic instances representing diverse cyberattack scenarios. The dataset was preprocessed through data cleaning, feature normalization, and dimensionality reduction before model training. Both Machine Learning and Deep Learning algorithms were trained and tested under the same experimental conditions to ensure a fair performance comparison. The evaluation was conducted using standard classification metrics, including Accuracy, Precision, Recall, and F1-score. The comparative analysis was further supported through performance visualization and a Flask-based deployment framework to validate the practical applicability of the proposed AI-driven cybersecurity solution.

B. Comparative Performance Analysis

Table I presents the comparative performance of the evaluated Machine Learning (ML) and Deep Learning (DL) models using the CICIDS2017 dataset. The results indicate that ensemble learning approaches consistently outperformed individual classifiers, with the proposed Voting Classifier achieving the highest accuracy of 99.6% among the ML models. Among the DL models, the LSTM network attained the best performance with an accuracy of 99.3%, demonstrating its capability to effectively capture sequential dependencies in network traffic. In contrast, conventional classifiers such as Logistic Regression and Gaussian Naïve Bayes exhibited comparatively lower predictive performance, highlighting the advantages of ensemble learning and deep neural architectures for cyberattack prediction.

Table.1 Performance Evaluation

Model	Accuracy	Precision	Recall	F1-Score
DT	0.985	0.985	0.984	0.984
RF	0.991	0.991	0.991	0.991
ETC	0.989	0.989	0.989	0.989
LR	0.907	0.908	0.907	0.904
GNB	0.876	0.882	0.876	0.874
Voting	0.996	0.996	0.996	0.996
DNN	0.980	0.980	0.980	0.980
CNN	0.984	0.985	0.984	0.984
LSTM	0.993	0.993	0.993	0.993
CNN + LSTM	0.990	0.990	0.990	0.990
CNN + LSTM + GRU	0.987	0.987	0.987	0.987

C. Performance Visualization

Figure 3 presents a graphical comparison of the performance achieved by the evaluated Machine Learning

and Deep Learning models based on Accuracy, Precision, Recall, and F1-score. The visualization provides a clear comparison of the predictive capabilities of all models and validates the numerical results reported in Table I. As observed, the proposed Voting Classifier achieved the highest performance among the Machine Learning models, while the LSTM network demonstrated superior results among the Deep Learning architectures. Hybrid deep learning models, including CNN–LSTM and CNN–LSTM–GRU, also exhibited competitive performance, outperforming standalone DNN and CNN models. Conversely, Logistic Regression and Gaussian Naïve Bayes produced comparatively lower evaluation metrics, indicating their limited capability to model the complex characteristics of modern network traffic. Overall, the graphical analysis confirms that ensemble learning and sequence-based deep learning architectures provide more accurate and reliable cyberattack prediction than conventional classification techniques.

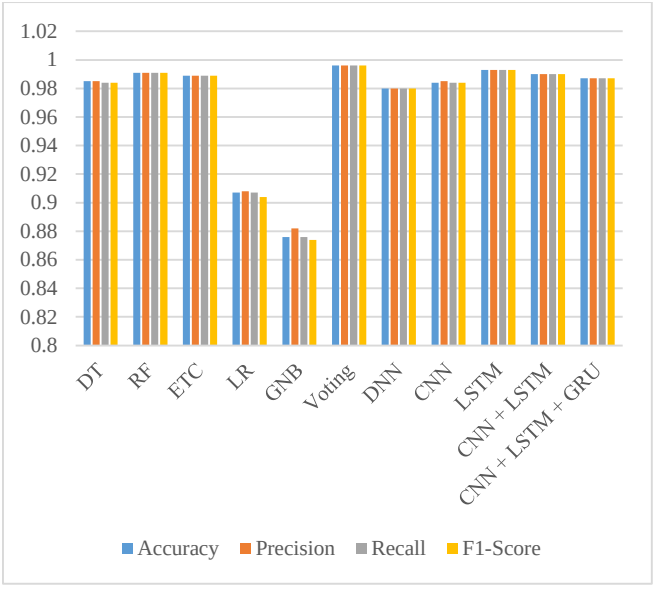


Fig. 3. Performance Comparison

D. Web-Based Deployment and Prediction Analysis

To validate the practical applicability of the proposed framework, the developed system was deployed as a Flask-based web application for real-time cyberattack prediction. The application enables users to upload network traffic data, perform automated prediction using the trained AI models, and receive comprehensive security insights through Explainable AI and Generative AI. The deployment workflow, illustrated in Figs. 4–6, demonstrates the complete prediction process from data input to attack analysis and recommended mitigation measures.

Fig. 4. Input Interface of the System

Figure 4 illustrates the input interface of the proposed application, where users can upload network traffic data for cyberattack analysis. The system automatically validates the input and performs the required preprocessing before forwarding the data to the prediction model.

Fig. 5. Cyber Attack Prediction Result

As shown in Fig. 5, the application displays the predicted attack category along with the corresponding confidence score after model inference. The prediction is generated using the trained AI model, enabling rapid identification of potential cyber threats.

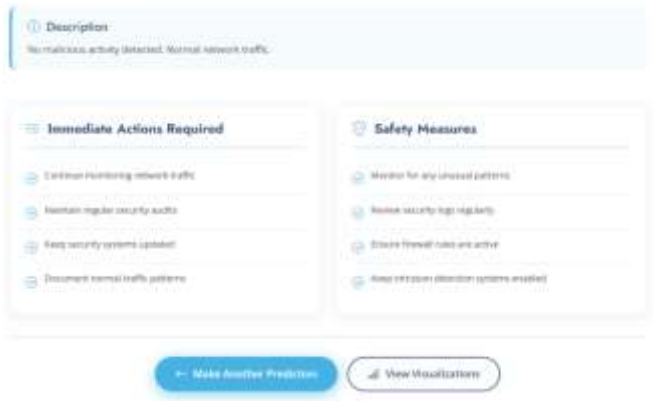


Fig. 6. Immediate Actions Required and Safety Measures

Figure 6 presents AI-generated recommendations based on the predicted cyberattack. The system provides immediate response actions, preventive security measures, and explanatory insights to assist users and security analysts in mitigating the identified threat effectively.

E. Discussion

The experimental results demonstrate the effectiveness of integrating traditional Machine Learning, Deep Learning, Generative AI, and Explainable AI for intelligent cyberattack prediction. As presented in Table I and Fig. 3, the proposed Voting Classifier achieved the highest performance among the ML models with an accuracy of 99.6%, while the LSTM model attained 99.3% accuracy among the DL models. The Flask-based deployment, illustrated in Figs. 4–6, further validates the practical applicability of the framework by enabling real-time attack prediction, AI-assisted threat interpretation, and actionable security recommendations. Although the framework demonstrates high predictive performance, its effectiveness depends on the availability of representative training data and periodic model updates to address evolving cyber threats. Future work will focus on incorporating emerging attack datasets, lightweight transformer

architectures, and adaptive continual learning techniques to further improve robustness and real-time cybersecurity intelligence.

CONCLUSION

The proposed AI-driven cybersecurity framework demonstrates the effectiveness of integrating Machine Learning, Deep Learning, Generative AI, and Explainable AI for accurate and interpretable cyberattack prediction. Using the CICIDS2017 dataset, the framework incorporated data preprocessing, feature normalization, and Principal Component Analysis (PCA) to improve data quality and model efficiency. A comprehensive evaluation of multiple ML and DL algorithms showed that the ensemble Voting Classifier (RF + LightGBM + XGBoost) achieved the highest performance among the ML models with an accuracy, precision, recall, and F1-score of 99.6%. Among the Deep Learning models, LSTM delivered the best performance with an accuracy of 99.3%, demonstrating its ability to effectively capture temporal dependencies in network traffic. Furthermore, the integration of Generative AI enhanced threat interpretation and security recommendation generation, while Explainable AI techniques, including SHAP and LIME, improved the transparency and trustworthiness of model predictions. The Flask-based deployment validated the practical applicability of the proposed framework by providing real-time cyberattack prediction, attack analysis, and user-friendly security insights. Overall, the proposed approach offers a scalable, accurate, and explainable solution for intelligent cybersecurity, making it suitable for deployment in modern network environments.

Future research will focus on developing adaptive cybersecurity frameworks capable of responding to evolving attack patterns through continual and online learning. The integration of advanced transformer-based models and agentic AI techniques can further improve contextual threat understanding and automated incident response. In addition, incorporating diverse real-world datasets, federated learning, and cloud-edge deployment will enhance scalability, privacy, and collaborative threat intelligence. These advancements will contribute to building robust, autonomous, and real-time cybersecurity systems for next-generation network infrastructures.

REFERENCES

1. R. von Solms and J. van Niekerk, “From information security to cyber security,” Computers & Security, vol. 38, pp. 97–102, Oct. 2013.
2. M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, “Survey of attack projection, prediction, and forecasting in cybersecurity,” IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 640–660, First Quarter 2019.
3. J. H. Li, “Cyber security meets artificial intelligence: A survey,” Frontiers of Information Technology & Electronic Engineering, vol. 19, no. 12, pp. 1462–1474, Dec. 2018.
4. I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, “Cybersecurity data science: An overview from machine learning perspective,” Journal of Big Data, vol. 7, no. 41, pp. 1–29, May 2020.
5. I. H. Sarker, M. H. Furhad, and R. Nowrozy, “AI-driven cybersecurity: An overview, security intelligence modeling and research directions,” SN Computer Science, vol. 2, no. 173, May 2021.
6. M. Ozkan-Okay, E. Akin, Ö. Aslan, S. Kosunalp, T. Iliev, and I. Beloev, “A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions,” IEEE Access, vol. 12, pp. 12229–12256, 2024.

7. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” Journal of Information Security and Applications, vol. 50, Art. no. 102419, Feb. 2020.
8. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep learning approach for intelligent intrusion detection system,” IEEE Access, vol. 7, pp. 41525–41550, 2019.
9. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, “On the effectiveness of machine and deep learning for cyber security,” in Proc. 10th Int. Conf. Cyber Conflict (CyCon), Tallinn, Estonia, 2018, pp. 371–390.
10. D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, “A survey of deep learning-based network anomaly detection,” Cluster Computing, vol. 22, Suppl. 1, pp. 949–961, Jan. 2019.
11. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” in Proc. 4th Int. Conf. Information Systems Security and Privacy (ICISSP), Funchal, Portugal, 2018, pp. 108–116.
12. S. M. Lundberg and S.-I. Lee, “A unified approach to interpreting model predictions,” in Advances in Neural Information Processing Systems (NeurIPS), vol. 30, 2017, pp. 4765–4774.
13. Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, “Explainable artificial intelligence applications in cyber security: State-of-the-art in research,” IEEE Access, vol. 10, pp. 93104–93139, 2022.
14. O. Arreche, T. R. Guntur, J. W. Roberts, and M. Abdallah, “E-XAI: Evaluating black-box explainable AI frameworks for network intrusion detection,” IEEE Access, vol. 12, pp. 23954–23988, 2024.
15. M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, “From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy,” IEEE Access, vol. 11, pp. 80218–80245, 2023.
16. S. Sai, U. Yashvardhan, V. Chamola, and B. Sikdar, “Generative AI for cyber security: Analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space,” IEEE Access, vol. 12, pp. 53497–53516, 2024.
17. I. H. Sarker, “Generative AI and large language modeling in cybersecurity,” in AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. Cham, Switzerland: Springer, 2024, pp. 79–99.
18. A. Dunmore, J. Jang-Jaccard, F. Sabrina, and J. Kwak, “A comprehensive survey of generative adversarial networks (GANs) in cybersecurity intrusion detection,” IEEE Access, vol. 11, pp. 76071–76094, 2023.
19. M. Al-Hawawreh and N. Moustafa, “Explainable deep learning for attack intelligence and combating cyber–physical attacks,” Ad Hoc Networks, vol. 153, Art. no. 103329, Feb. 2024.
20. Y. Kim, G. Dán, and Q. Zhu, “Human-in-the-loop cyber intrusion detection using active learning,” IEEE Transactions on Information Forensics and Security, vol. 19, pp. 8658–8672, 2024.