Cyber Attack Prediction using Traditional Methods, Machine Learning and Gen AI: A Conceptual Framework

Komal P. Kanojia, PhD
Associate Professor, Dept. of Computer Engineering
Sandip Institute of Technology and Research Centre, Nashik

Urmila U. Ghare
B.Tech, Dept. of Computer Engineering
Sandip Institute of Technology and Research Centre, Nashik

Sakshi G. Pawar
B.Tech, Dept. of Computer Engineering
Sandip Institute of Technology and Research Centre, Nashik

Sharayu S. Shewale
B.Tech, Dept. of Computer Engineering
Sandip Institute of Technology and Research Centre, Nashik

Pooja P. Satpute
B.Tech, Dept. of Computer Engineering
Sandip Institute of Technology and Research Centre, Nashik

ABSTRACT
The advancements in cyberattacks pose threats and challenges for individuals and organizations in protecting sensitive information and maintaining secure network infrastructures. Traditional security methods like firewalls, signature-based intrusion detection systems (IDSs) are effective against known threats but struggle to detect sophisticated and unseen attacks. Machine learning techniques can improve cyberattack prediction by detecting patterns in network traffic. However, many ML models provide limited explanations, making it difficult for security analysts to understand and respond to predictions effectively. Generative AI offers effective approaches to improve cybersecurity by generating human-readable explanations, summarizing threats, and recommending mitigation strategies. This paper proposes a framework that integrates traditional cybersecurity methods, machine learning, and Generative AI to support intelligent cyberattack prediction. The prediction component of the proposed framework is evaluated on the NSL-KDD benchmark using five machine learning models, a rule-based baseline, and a hybrid detector. The results show a substantial gap between cross-validation and official test performance, while the hybrid detector improves the F1-score compared with Random Forest alone. The explainability, risk interpretation, and Generative AI components are proposed as parts of the conceptual framework and remain to be experimentally evaluated.

General Terms
Security, Algorithms, Machine Learning, Artificial Intelligence

Keywords
Cybersecurity, cyberattack prediction, machine learning, generative artificial intelligence, Threat intelligence, risk assessment, decision support system

1. INTRODUCTION
The rapid growth of digital technologies has changed how organizations store, process, and exchange information. Cloud computing, mobile applications, and online banking improved connectivity but also created new opportunities for attackers. Cyberattacks such as ransomware, DDoS, phishing, malware, and zero-day attacks are becoming more frequent and sophisticated, and can interrupt critical services, cause financial loss, and damage reputation [1],[2]. This indicates the need for intelligent and proactive security systems.

For decades, cybersecurity has relied on intrusion detection systems, firewalls, and antivirus tools that identify known attacks using predefined rules and signatures. Because they depend on previously recorded attack information, they struggle to detect new, modified, and evolving threats [3], which delays incident response.

1.1 Machine Learning for Cyber Attack Prediction
Machine learning (ML) can examine large volumes of network traffic, identify hidden patterns, and distinguish legitimate from malicious activity. Supervised techniques such as Decision Tree, Logistic Regression, Random Forest, K-Nearest Neighbors (KNN), and Support Vector Machine (SVM) are widely used, and deep learning models such as CNNs, RNNs, and LSTM networks have also been explored [4],[5],[6]. Generative adversarial networks [7] and GAN-based models like TadGAN [8] have been applied to intrusion and anomaly detection.

However, many ML models operate as black boxes that give a prediction without a clear reason, which reduces analyst trust and complicates incident response [9],[10]. Models also degrade in new environments, under evolving attack patterns, or with imbalanced data [11], and suffer from high false-positive rates and dependence on high-quality labeled data.

1.2 Generative AI for Interpretability
Large Language Models (LLMs) and other generative AI techniques can turn technical prediction results into human-readable explanations, summarize security events, assist threat analysis, and suggest mitigation measures [12],[13]. GenAI is not meant to replace ML-based prediction; it can act as an additional layer that explains outputs and supports security professionals in decision-making.

1.3 Research Motivation
Traditional mechanisms, machine learning, explainable AI, and Generative AI have been studied extensively but mostly separately [1]. Most works either improve the accuracy of conventional and deep learning methods or compare approaches for predicting attacks [14],[15],[16],[17], and very few discuss a framework that integrates attack prediction with justification, risk assessment, and security recommendations. This paper addresses this gap with a structured blueprint for future development and validation.

1.4 Contributions

The main contributions of this paper are:

- A review of traditional, machine learning, and Generative AI methods for cyberattack prediction, with the key research gaps.
- A conceptual framework integrating traditional methods, machine learning, explainability, and Generative AI in one architecture.
- An experimental study on NSL-KDD of five ML models, a rule-based baseline, and a hybrid detector, with seen versus unseen attack analysis, and a discussion of challenges and ethical considerations.

The paper covers related work (Section 2), gaps (3), the framework (4), experiments (5, 6), and challenges and conclusions (7, 8).

2. LITERATURE REVIEW

This section reviews ten selected studies, grouped by main contribution and compared in Table 1.

2.1 Traditional and Machine Learning-Based Detection

Shaukat *et al.* [3] surveyed 312 works on machine learning for cybersecurity and showed the shift from reactive, signature-based detection to data-driven detection, but offered no framework for acting on predictions. Bou Nassif *et al.* [18] reviewed 290 studies on ML-based anomaly detection and found that training-data quality, class distribution, and representativeness strongly affect detection performance and generalization.

Al-Quayed *et al.* [19] proposed a situation-based predictive approach for intrusion detection in Industry 4.0 wireless sensor networks using ML and DL, but it is specific to that environment.

2.2 Advanced Cyber Attack Prediction

Vinayakumar *et al.* [4] proposed Scale-Hybrid-IDS-AlertNet, a deep-neural-network approach for network- and host-level events in large-scale monitoring. It needs extensive data and computing resources, and its predictions are hard for analysts to interpret.

Tserenkhuu *et al.* [14] built an intrusion detection system for SDN-based IoT networks using deep neural networks with XAI-based feature selection and domain-specific features, maintaining accuracy with simpler models; however, XAI is used only internally and not to explain individual alerts.

2.3 Explainable AI for Cybersecurity

Arreche *et al.* [9] compared SHAP and LIME across seven AI models and three intrusion-detection datasets and found that explanation quality varies with model and dataset, so no single technique is consistently best.

Together, [9] and [14] show the value of XAI but remain model-oriented: explanations are not delivered as analyst-facing output with context, risk assessment, and recommended actions, which the proposed framework targets.

2.4 Generative AI for Cybersecurity

Gupta *et al.* [12] examined Generative AI in cybersecurity and privacy, showing its usefulness for analysis and natural-language explanation as well as dual-use risks such as phishing.

Ozkan-Okay *et al.* [20] reviewed AI/ML techniques for cybersecurity and the emerging role of Generative AI, noting persistent concerns about reliability, security, and misuse.

Ferrag *et al.* [21] proposed a privacy-preserving BERT-based lightweight model for threat detection in IoT/IIoT, but it focuses on detection rather than a workflow linking prediction with GenAI explanation and recommendations.

Ankalaki *et al.* [1] reviewed the evolution of cyberattack prediction from traditional ML to Generative AI; as a review, it does not implement an end-to-end architecture.

Table 1. Comparison of Existing Studies

Author(s), Year, Ref	Methodology and Domain	Key Findings	Limitation / Gap
Ankalaki et al., 2025 [1]	Review of ML, DL, XAI, NLP, and GenAI for cyberattack prediction.	GenAI can complement ML and DL in cybersecurity.	No specific end-to-end architecture is proposed.
Shaukat et al., 2020 [3]	Survey of 312 ML studies in cybersecurity.	Highlights limitations of reactive detection and outdated datasets.	No mechanism for post-prediction security action.
Vinayakumar et al., 2019 [4]	Scalable DNN-based IDS using network and host data.	Supports large-scale and real-time intrusion detection	Requires substantial data and computation; limited interpretability.
Arreche et al., 2024 [9]	Evaluation of SHAP and LIME across AI models and IDS datasets.	XAI performance varies across models and datasets.	Explanations remain mainly model-oriented.
Gupta et al., 2023 [12]	Study of GenAI applications and risks in cybersecurity.	GenAI supports explanations and mitigation suggestions.	Not integrated with an upstream prediction model.
Tserenkhuu et al., 2025 [14]	DL and XAI for SDN-based IoT intrusion detection.	XAI-based feature selection improves model efficiency.	XAI is mainly used internally.
Bou Nassif et al., 2021 [18]	Review of 290 ML-based anomaly detection studies.	Data quality and class balance strongly affect detection.	Review-based study without GenAI integration.
Al-Quayed et al., 2024 [19]	Situation-based ML/DL intrusion prediction for Industry 4.0 WSN.	Context-based analysis improves intrusion prioritization.	Limited to WSN and Industry 4.0; no GenAI.
Ozkan-Okay et al., 2024 [20]	Survey of AI, ML, RL, and ChatGPT applications in cybersecurity.	GenAI can assist security tasks but introduces risks.	No integrated prediction and GenAI framework.
Ferrag et al., 2024 [21]	Lightweight BERT-based threat detection for IoT/IIoT.	Demonstrates efficient LLM-based threat detection.	Focuses on detection rather than explanation and recommendations.

3. RESEARCH GAP ANALYSIS

The ten studies show limited integration of prediction, interpretation, deployment, and decision-making, rather than a lack of individual techniques.

3.1 Interpretation and Response Gaps

ML approaches mainly identify or classify malicious activity, while XAI is often used for feature selection or technical interpretation, leaving a gap between predictions and explanations that analysts can understand. Studies also show limited integration of prediction with risk assessment and

security recommendations, creating a gap between attack identification and response.

3.2 Generalization Across Security Environments

Many approaches target specific environments such as IoT, SDN, Industry 4.0, and NextG networks [19],[21],[22], and ML has been applied to vulnerability analysis in industrial IoT under its own constraints [23]. Performance also depends on data quality, class balance, feature selection, and changing attack patterns, so a more adaptable architecture is needed.

3.3 Generative AI Reliability and Fragmented Intelligence

Generative AI can support analysis and natural-language assistance, but its outputs may be inaccurate or misused [12],[20], so privacy, security, and reliability concerns require output validation and human oversight. Moreover, ML, XAI, and Generative AI offer complementary capabilities that are not consistently integrated into a unified workflow from network data to risk-aware reporting [24].

4. PROPOSED CONCEPTUAL FRAMEWORK

The proposed framework integrates ML-based cyberattack prediction, explainability, and Generative AI-assisted analysis into a unified workflow for prediction, interpretation, risk assessment, and security recommendations. The architecture is shown in Figure 1 and the detailed workflow in Figure 2.

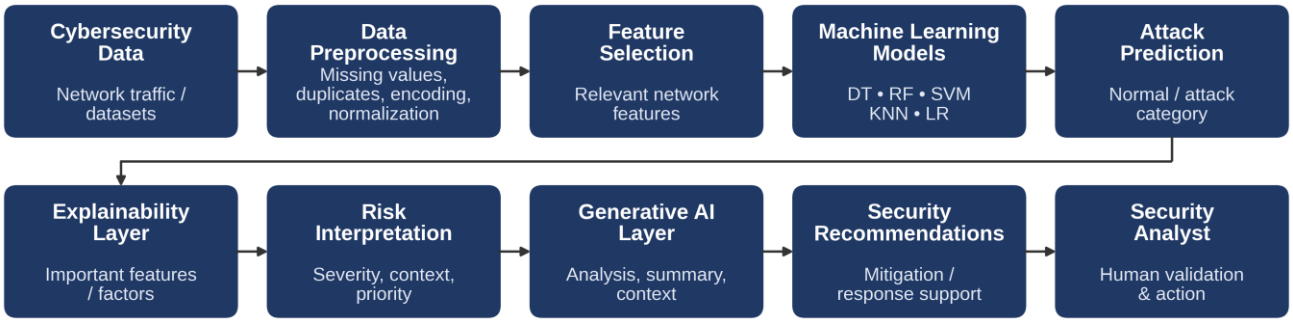


Figure 1: End-to-end proposed conceptual framework for ML-based cyberattack prediction and Generative AI-assisted security analysis.

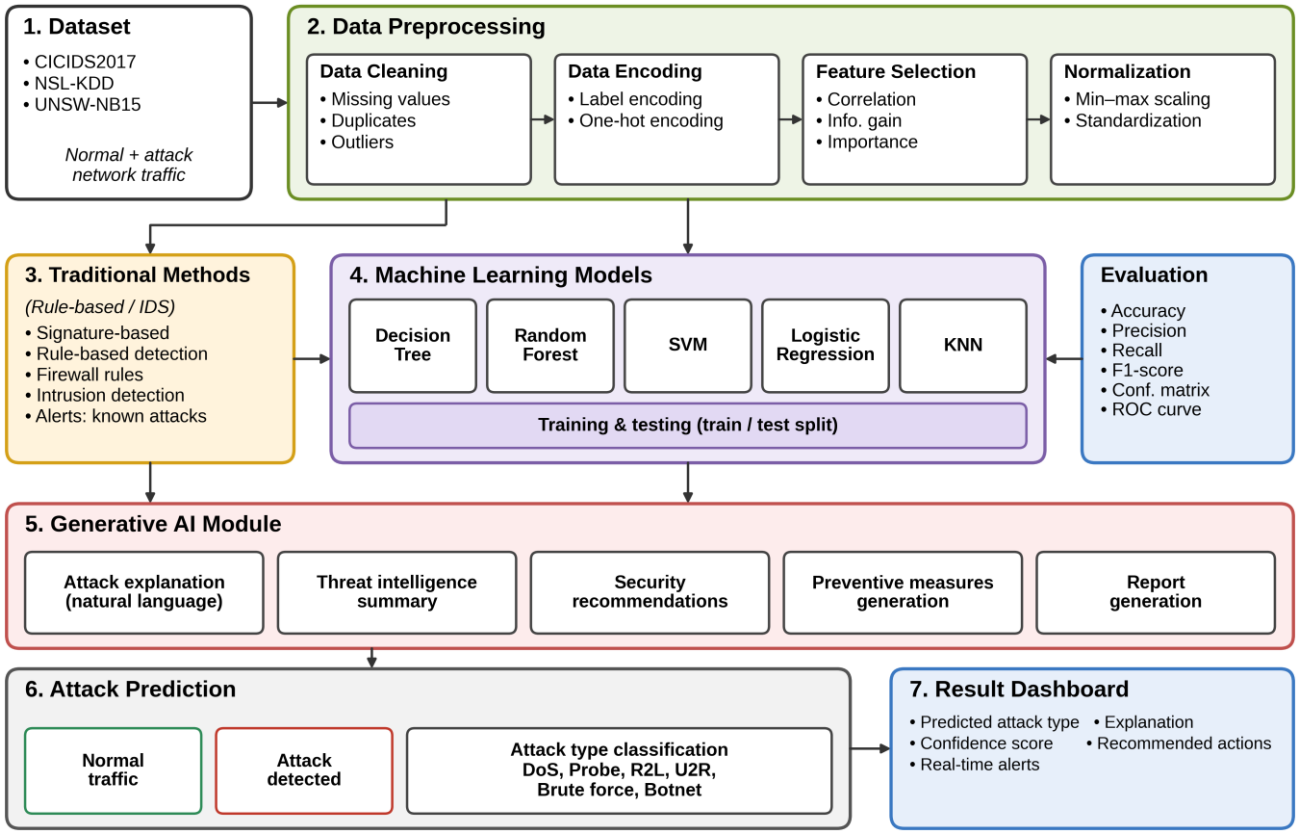


Figure 2. Workflow of the proposed conceptual framework; only the prediction stage is evaluated in Sections 5 and 6.

4.1 Data Processing and Feature Selection

The framework collects data from network traffic or benchmark datasets such as CICIDS2017, NSL-KDD, or UNSW-NB15 [25]. Preprocessing removes duplicates, handles missing values, converts categorical data to numerical form,

and normalizes features; feature selection then keeps the network features most useful for attack prediction.

4.2 Machine Learning-Based Prediction

The preprocessed data is given to models such as Decision Tree, Random Forest, SVM, KNN, and Logistic Regression, which classify activity as normal or attack.

4.3 Explainability and Risk Interpretation

An explainability component identifies the features that contribute most to each decision; these are analyzed with the attack category to interpret the associated risk. Explanations and risk interpretations support analysts rather than replace expert judgment, and the choice and validation of a specific explainability method and risk-scoring procedure remain future work.

4.4 Generative AI Layer

Prediction and explanation outputs, with relevant context, are passed to the Generative AI layer, which acts as a supporting component: it translates technical results into natural language, summarizes the detected threat, and recommends security measures.

4.5 Security Analyst and Human Validation

The final information is presented to the security analyst [24],[26]. Human validation is essential because GenAI responses may be inaccurate or incomplete and must be verified before implementation.

5. EXPERIMENTAL SETUP AND EVALUATION STRATEGY

The prediction stage of the framework was evaluated on the NSL-KDD benchmark [27] using scikit-learn [28].

5.1 Data and Preprocessing

NSL-KDD has an official training set (125,973 records) and test set (22,544 records) with 41 features. Classes (train / test): Normal 67,343 / 9,711, DoS 45,927 / 7,460, Probe 11,656 / 2,421, R2L 995 / 2,885, U2R 52 / 67. The main task is binary (Normal vs. Attack); the four attack categories are used only for the breakdown in Section 6.3. Categorical features were one-hot encoded (122 features in total) and all features were min–max scaled using training data only. The test set contains 17 attack types that are absent from training (3,750 of 12,833 attacks, 29.2%), so it imitates previously unseen threats.

5.2 Models and Baselines

Decision Tree, Random Forest (100 trees), SVM (RBF kernel, trained on a 30,000-record subsample to limit computational cost), Logistic Regression and KNN (k = 5) were trained on all 122 features with default scikit-learn settings (seed 42); because of the subsample, the SVM comparison is not strictly equivalent. A rule-based baseline stands for the traditional layer: eight fixed thresholds on error rates, connection counts, failed logins and root shells, which encode general DoS, Probe, R2L and U2R indicators rather than attack signatures and were fixed before test evaluation. Default settings and the official split follow the standard NSL-KDD protocol [27]. The hybrid detector raises an alert when either Random Forest or the rules do.

5.3 Metrics

We report accuracy, precision, recall, F1-score, ROC-AUC and false-positive rate (FPR) on the test set (attack = positive class), and 5-fold stratified cross-validation on the training data (scaling fitted inside each fold). Explainability (e.g., SHAP and LIME [9], [29], [30], [31]) will be assessed by feature-ranking stability, agreement between methods, and the performance drop when top features are removed. The GenAI layer will be rated by analysts for correctness, relevance, clarity and actionability, with an automatic check that its attack category, features and risk level match the ML output; this is future work and not reported here.

6. RESULTS AND ANALYSIS

6.1 Overall Performance

Table 2, Figure 3 and Figure 4 compare all methods on the test set. The ML models reach high precision (0.92–0.97) but low recall (0.62–0.69), so 31–38% of attacks are missed. Random Forest has the best AUC (0.960) and lowest FPR (2.7%); the Decision Tree has the best ML accuracy (0.790). The simple rule baseline (accuracy 0.795) performs on par with, or slightly better than, the ML models. The hybrid detector gives the best accuracy (0.843), recall (0.790) and F1-score (0.851), against an F1-score of 0.757 for Random Forest alone. It cuts missed attacks from 4,854 to 2,698, but raises false alarms from 266 to 851 (FPR 2.7% to 8.8%). The hybrid detector improves recall and F1-score compared with Random Forest alone, but increases the false-positive rate. Therefore, its suitability depends on the balance between minimizing missed attacks and controlling false alarms.

Table 2. Performance on the Test Set, All 122 Features (Best in Bold)

Method	Acc.	Prec.	Rec.	F1	AUC	FPR
Decision Tree	0.790	0.919	0.692	0.790	0.806	0.080
Random Forest	0.773	**0.968**	0.622	0.757	**0.960**	**0.027**
SVM (RBF)	0.767	0.920	0.646	0.759	0.823	0.074
Logistic Reg.	0.754	0.917	0.624	0.743	0.827	0.075
KNN (k=5)	0.769	0.924	0.648	0.762	0.829	0.070
Rule-based	0.795	0.926	0.696	0.795	–	0.073
Hybrid (RF+rules)	**0.843**	0.923	**0.790**	**0.851**	–	0.088

FPR = false-positive rate (lower is better). AUC is not reported for the rule-based and hybrid detectors because continuous prediction scores were not available.

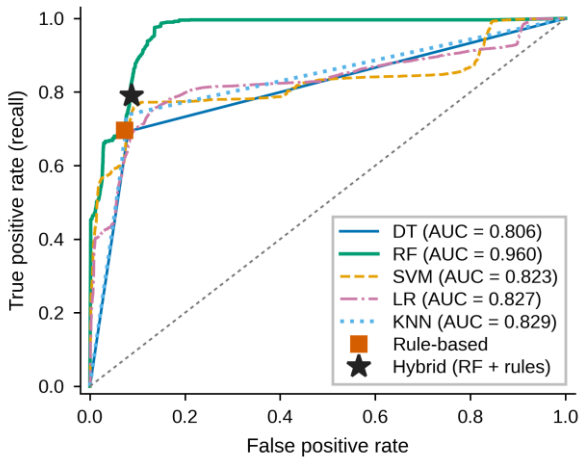


Figure 3: ROC curves of the ML models; markers show the rule-based and hybrid operating points.

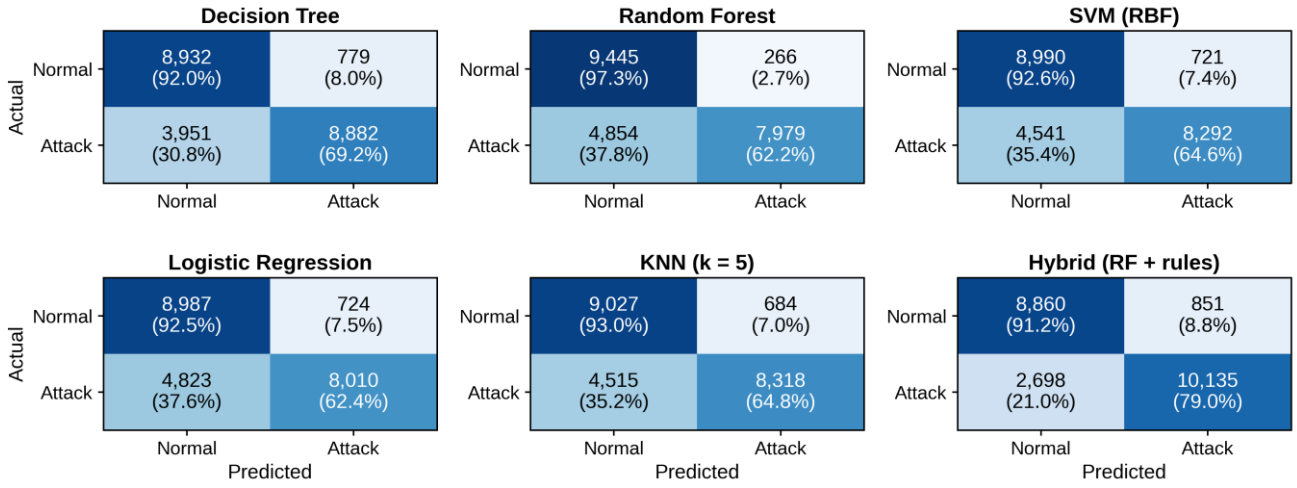


Figure 4: Confusion matrices on the test set (counts and row percentages).

6.2 Cross-Validation versus Test Set

Cross-validated accuracy is very high (0.973–0.998), yet accuracy on the official test set is 0.21–0.23 lower for every model (Table 3). Random cross-validation folds may contain attack types also represented in the corresponding training folds. Therefore, cross-validation may not fully reflect performance on attack types absent from training.

Table 3. Cross-Validation vs. Test Accuracy (All 122 Features)

Model	CV acc. (mean ± s.d.)	CV F1	Test acc.	Gap
Decision Tree	0.9973 ± 0.0003	0.9971	0.7902	0.207
Random Forest	0.9983 ± 0.0002	0.9981	0.7729	0.225
SVM (RBF)	0.9835 ± 0.0011	0.9823	0.7666	0.217
Logistic Reg.	0.9725 ± 0.0010	0.9702	0.7539	0.219
KNN (k=5)	0.9960 ± 0.0003	0.9957	0.7694	0.227

Gap = cross-validation accuracy − test accuracy (Table 2).

6.3 Attack Categories and Unseen Attacks

Figure 5 shows Random Forest detection rates by attack category and for seen versus unseen attack types. Random Forest detects most DoS (79%) and Probe (76%) attacks but few R2L (8%) and U2R (12%) attacks, which are rare in training. It also detects 77.7% of attacks of seen types but only 24.7% of unseen ones. The rule baseline drops far less (72.0% to 63.7%), because its indicators describe general behaviour instead of known signatures. The hybrid detector reaches 84.1% and 66.7%. On this dataset, these results are consistent with the idea that traditional methods and machine learning complement each other. These results demonstrate generalization performance on attack types absent from the training set within NSL-KDD. They should not be interpreted as proof of reliable detection of real-world zero-day attacks.

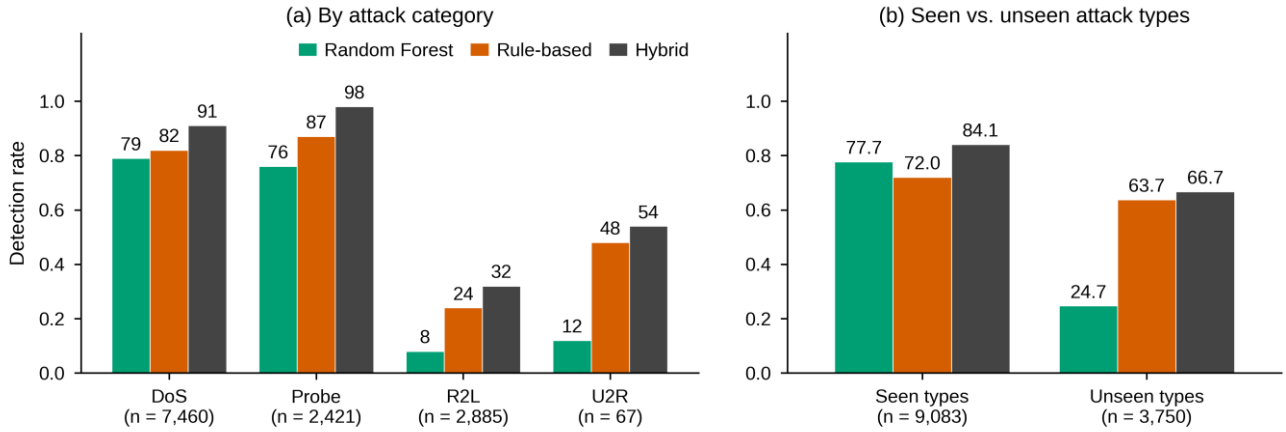


Figure 5: Detection rates on the test set: (a) by attack category; (b) seen versus unseen attack types.

6.4 Feature Selection and Limitations

A preliminary feature-selection experiment retained the 20 highest-ranked features using mutual information computed on the training set. This reduced Random Forest training time from 12.6 s to 7.9 s, but decreased the test F1-score of every model by 2.2–5.7 percentage points; therefore, all 122 features were retained for the reported experiments. Per-model F1-score comparisons under feature selection, SHAP/LIME ranking stability, and analyst-based evaluation of Generative AI outputs are left for future work. Other limitations include the use of a dated benchmark dataset, default model settings, a single train-test split, an SVM trained on a subsample, and manually specified rule thresholds. Tuning, repeated splits, additional datasets, and evaluation of the explainability and Generative AI components are planned.

7. CHALLENGES AND RESPONSIBLE USE

Several challenges must be addressed before practical implementation. ML prediction can be affected by data quality,

class imbalance, changing attack patterns, and false predictions [32],[33], and adopting AI-based security tools brings operational challenges [34]. Explainability techniques may also vary in effectiveness across models and datasets.

Generative AI adds concerns of inaccurate outputs, privacy risks, prompt manipulation, and misuse, so generated explanations and recommendations should be validated against reliable security information. Human supervision for high-risk decisions, data protection, output verification, access controls, and continuous model evaluation should be part of any implementation.

8. CONCLUSION

This paper introduced a framework that integrates traditional cybersecurity methods, machine learning, explainability, and Generative AI-assisted analysis into a unified workflow for cyberattack prediction. The review of ten studies revealed gaps between prediction and interpretation, prediction and response, generalization across environments, and the reliability and governance of Generative AI.

Experiments on NSL-KDD showed that models with cross-validated accuracy above 97% achieved only 75–79% accuracy on the official test set, highlighting challenges in generalization to unseen attack types. The hybrid approach combining Random Forest and the rule-based baseline achieved a recall of 0.790 and an F1-score of 0.851, with a higher false-positive rate (8.8%). However, these experiments evaluate the prediction component, not the complete framework. Future work should evaluate the framework on additional datasets, investigate real-time deployment and adversarial robustness, and assess the correctness and usefulness of Generative AI-generated explanations and recommendations with security analysts.

9. REFERENCES

[1] Ankalaki, S., Atmakuri, A. R., Pallavi, M., Hukkeri, G. S., Jan, T., and Naik, G. R. 2025. Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence. IEEE Access, vol. 13, pp. 44662–44706. DOI: 10.1109/ACCESS.2025.3547433.

[2] Gorment, N. Z., Selamat, A., Cheng, L. K., and Krejcar, O. 2023. Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges, and Future Directions. IEEE Access, vol. 11, pp. 141045–141089. DOI: 10.1109/ACCESS.2023.3256979.

[3] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., and Xu, M. 2020. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. IEEE Access, vol. 8, pp. 222310–222354. DOI: 10.1109/ACCESS.2020.3041951.

[4] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., and Venkatraman, S. 2019. Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, vol. 7, pp. 41525–41550. DOI: 10.1109/ACCESS.2019.2895334.

[5] Anis, F. M., Alabdullatif, M., Aljbli, S., and Hammoudeh, M. 2025. A Survey on the Applications of Deep Learning in Network Intrusion Detection Systems to Enhance Network Security. IEEE Access, vol. 13, pp. 185357–185373. DOI: 10.1109/ACCESS.2025.3624952.

[6] Lucas, T. J., et al. 2023. A Comprehensive Survey on Ensemble Learning-Based Intrusion Detection Approaches in Computer Networks. IEEE Access, vol. 11, pp. 122638–122676. DOI: 10.1109/ACCESS.2023.3328535.

[7] Dunmore, A., Jang-Jaccard, J., Sabrina, F., and Kwak, J. 2023. A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection. IEEE Access, vol. 11, pp. 76071–76094. DOI: 10.1109/ACCESS.2023.3296707.

[8] Geiger, A., Liu, D., Alnegheimish, S., Cuesta-Infante, A., and Veeramachaneni, K. 2020. TadGAN: Time Series Anomaly Detection Using Generative Adversarial Networks. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, pp. 33–43. DOI: 10.1109/BigData50022.2020.9378139.

[9] Arreche, O., Guntur, T. R., Roberts, J. W., and Abdallah, M. 2024. E-XAI: Evaluating Black-Box Explainable AI Frameworks for Network Intrusion Detection. IEEE Access, vol. 12, pp. 23954–23988. DOI: 10.1109/ACCESS.2024.3365140.

[10] Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., and Taher, F. 2022. Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. IEEE Access, vol. 10, pp. 93104–93139. DOI: 10.1109/ACCESS.2022.3204051.

[11] Jamal, M. H., Naz, N., Khattak, M. A. K., Saeed, F., Altamimi, S. N., and Qasem, S. N. 2023. A Comparison of Re-Sampling Techniques for Detection of Multi-Step Attacks on Deep Learning Models. IEEE Access, vol. 11, pp. 127446–127457. DOI: 10.1109/ACCESS.2023.3332512.

[12] Gupta, M., Akiri, C., Aryal, K., Parker, E., and Praharaj, L. 2023. From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. IEEE Access, vol. 11, pp. 80218–80245. DOI: 10.1109/ACCESS.2023.3300381.

[13] Hasanov, I., Virtanen, S., Hakkala, A., and Isoaho, J. 2024. Application of Large Language Models in Cybersecurity: A Systematic Literature Review. IEEE Access, vol. 12, pp. 176751–176778. DOI: 10.1109/ACCESS.2024.3505983.

[14] Tserenkhuu, M., Hossain, M. D., Taenaka, Y., and Kadobayashi, Y. 2025. Intrusion Detection System Framework for SDN-Based IoT Networks Using Deep Learning Approaches With XAI-Based Feature Selection Techniques and Domain-Constrained Features. IEEE Access, vol. 13, pp. 136864–136880. DOI: 10.1109/ACCESS.2025.3595595.

[15] Okutan Kara, A., Kara, M., and Boyaci, A. 2025. A Comparative Analysis of Machine Learning and Deep Reinforcement Learning Approaches for Adaptive Intrusion Detection. IEEE Access, vol. 13, pp. 189833–189849. DOI: 10.1109/ACCESS.2025.3627098.

[16] Lee, S., Lee, K., Cho, S., and Choi, C. 2025. APTStop: A Real-Time Framework for APT Defense via Strategic Threat Observation and Prediction. IEEE Access, vol. 13, pp. 183134–183155. DOI: 10.1109/ACCESS.2025.3624035.

[17] Verma, P., Lemley, J., Schukat, M., O'Shea, D., and Newe, T. 2026. CRISP: Cyber-Resilient Intelligent Systems for Predicting Threats in Digital Ecosystems. IEEE Access, vol. 14, pp. 15841–15868. DOI: 10.1109/ACCESS.2026.3658507.

[18] Nassif, A. B., Talib, M. A., Nasir, Q., and Dakalbab, F. M. 2021. Machine Learning for Anomaly Detection: A Systematic Review. IEEE Access, vol. 9, pp. 78658–78700. DOI: 10.1109/ACCESS.2021.3083060.

[19] Al-Quayed, F., Ahmad, Z., and Humayun, M. 2024. A Situation-Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0. IEEE Access, vol. 12. DOI: 10.1109/ACCESS.2024.3372187.

[20] Ozkan-Okay, M., Akin, E., Aslan, O., Kosunalp, S., Iliev, T., Stoyanov, I., and Beloev, I. 2024. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access, vol. 12, pp. 12229–12256. DOI: 10.1109/ACCESS.2024.3355547.

[21] Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., Lestable, T., and Thandi, N. S. 2024. Revolutionizing Cyber Threat Detection With Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices. IEEE Access, vol. 12, pp. 23733–23750. DOI: 10.1109/ACCESS.2024.3363469.

[22] Hossain, M. J., Alam, K., Monir, M. F., Hoque, M. M., and Ahmed, T. 2025. Explainable AI Meets Synthetic Data: A Deep Learning Framework for Detecting Network Intrusion in NextG Network Infrastructure. IEEE Access, vol. 13. DOI: 10.1109/ACCESS.2025.3585783.

[23] Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., and Jain, R. 2019. Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822–6834, Aug. 2019. DOI: 10.1109/JIOT.2019.2912022.

[24] Binbeshr, F., Imam, M., Ghaleb, M., Hamdan, M., Rahim, M. A., and Hammoudeh, M. 2025. The Rise of Cognitive SOCs: A Systematic Literature Review on AI Approaches. IEEE Open Journal of the Computer Society, vol. 6. DOI: 10.1109/OJCS.2025.3536800.

[25] De Keersmaeker, F., Cao, Y., Ndonda, G. K., and Sadre, R. 2023. A Survey of Public IoT Datasets for Network Security Research. IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1808–1840, third quarter 2023. DOI: 10.1109/COMST.2023.3288942.

[26] Vielberth, M., Böhm, F., Fichtinger, I., and Pernul, G. 2020. Security Operations Center: A Systematic Study and Open Challenges. IEEE Access, vol. 8, pp. 227756–227779. DOI: 10.1109/ACCESS.2020.3045514.

[27] Tavallaee, M., Bagheri, E., Lu, W., and Ghorbani, A. A. 2009. A Detailed Analysis of the KDD CUP 99 Data Set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, pp. 1–6. DOI: 10.1109/CISDA.2009.5356528.

[28] Pedregosa, F., et al. 2011. Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research, vol. 12, pp. 2825–2830.

[29] Yang, T., Qiao, Y., and Lee, B. 2024. Explaining Probabilistic Bayesian Neural Networks for Cybersecurity Intrusion Detection. IEEE Access, vol. 12, pp. 97004–97016. DOI: 10.1109/ACCESS.2024.3421330.

[30] Barnard, P., Marchetti, N., and DaSilva, L. A. 2022. Robust Network Intrusion Detection Through Explainable Artificial Intelligence (XAI). IEEE Networking Letters, vol. 4, no. 3, pp. 167–171, Sep. 2022. DOI: 10.1109/LNET.2022.3186589.

[31] Kundu, P. P., Truong-Huu, T., Chen, L., Zhou, L., and Teo, S. G. 2022. Detection and Classification of Botnet Traffic Using Deep Learning With Model Explanation. IEEE Transactions on Dependable and Secure Computing, early access, June 15, 2022. DOI: 10.1109/TDSC.2022.3183361.

[32] Zhen, L., Kamarudin, N. H., Kok, V. J., and Qamar, F. 2025. Anomaly Detection Model in Network Security Situational Awareness Based on Machine Learning: Limitation, Techniques, and Future Trends. IEEE Access, vol. 13, pp. 126084–126129. DOI: 10.1109/ACCESS.2025.3589620.

[33] Ennaji, S., De Gaspari, F., Hitaj, D., Kbidi, A., and Mancini, L. V. 2025. Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects. IEEE Access, vol. 13, pp. 148613–148645. DOI: 10.1109/ACCESS.2025.3600984.

[34] Chan, L., et al. 2019. Survey of AI in Cybersecurity for Information Technology Management. In Proceedings of the 2019 IEEE Technology & Engineering Management Conference (TEMSCON), Atlanta, GA, USA, pp. 1–8. DOI: 10.1109/TEMSCON.2019.8813605.

[35] Devendra Singh Kushwaha, Prof. Ashish Khare and Dr. J. L. Rana "Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET" has been published in International Journal of Computer Applications IJCA (0975 – 8887) Volume 62– No.7, January 2013,pp21-25.

[36] Devendra Singh Kushwaha, Divya Kishor Sapkale, Kumudini Kishor Khairnar, Sonakshi Sopan Kanse, Mansi Nilkanth Bhole . Neural-XGB Fusion: A Hybrid Approach for Disaster Prediction and Management using Machine Learning. International Journal of Computer Applications. 187, 144 (Sep 2026), 27-35. DOI=10.5120/ijcaaefd60e28e07