Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 28 No. 7s (2025)

Cyber Attack Detection Using a Supervised ML Techniques

Ms. Priyanka Patani[1], Dr. Dushyantsinh Rathod[2]

[1]PhD Scholar, Computer Engineering, Gandhinagar University, Gujarat, India,priyankapatani1295@gmail.com

[2]Professor & HOD(CSE), GIT, Gandhinagar University, Gujarat,India.dushyantsinh.rathod@gmail.com

Article History:

Received: 08-11-2025

Revised: 17-12-2025

Accepted: 26-12-2025

Abstract:

Introduction: The rapid growth of digital technologies and interconnected systems has significantly increased the risk of cyberattacks across networks and information infrastructures. Traditional signature-based intrusion detection systems often fail to identify sophisticated and zero-day attacks. Supervised machine learning techniques provide an effective solution by learning patterns from labeled historical data to distinguish between normal and malicious activities. These models can analyze large volumes of network traffic and system logs with improved accuracy and adaptability. Therefore, supervised machine learning has emerged as a powerful approach for enhancing cyberattack detection and strengthening cybersecurity defenses.

Objectives: The primary objective of this study is to develop an effective cyberattack detection system using supervised machine learning techniques. It aims to train and evaluate various classification algorithms to accurately distinguish between normal and malicious network activities. The study seeks to compare the performance of different supervised models using metrics such as accuracy, precision, recall, and F1-score. Another objective is to identify the most efficient model with minimal false positives and false negatives.

Methods: The hybrid ensemble–based cyber attack detection methodology integrates data preprocessing, feature optimization, multiple classifiers, and ensemble learning to deliver a high-performance and adaptive cyber security solution capable of identifying both known and emerging threats effectively.

Results: The experimental results demonstrate that supervised machine learning models effectively detect cyberattacks with high accuracy and reliability. Among the evaluated algorithms, ensemble methods achieved superior performance compared to individual classifiers. The models showed strong detection rates with reduced false positives and improved overall classification metrics. These findings confirm that supervised learning techniques significantly enhance cyberattack detection capability in modern cybersecurity systems.

Conclusions: The study concludes that supervised machine learning techniques provide an efficient and reliable approach for cyberattack detection. The evaluated models demonstrated strong classification performance, particularly ensemble methods, in identifying malicious activities. Proper feature selection and data preprocessing further enhance detection accuracy and reduce false alarms. Overall, supervised learning-based systems offer a scalable and robust solution for strengthening modern cybersecurity defenses.

Keywords: Cyber Attack Detection, Supervised Machine Learning, Intrusion Detection System (IDS), Network Security, Classification Algorithms, Random Forest, Support Vector Machine (SVM), XGBoost, Cybersecurity Analytics, Threat Detection.

1. Introduction

The rapid growth of information technology, cloud services, Internet of Things (IoT), and large-scale computer networks has significantly increased the vulnerability of digital systems to cyber attacks. Modern cyber threats such as denial-of-service attacks, malware, ransomware, phishing, and advanced persistent threats have become more frequent, complex, and difficult to detect. Conventional security solutions, including firewalls and signature-based intrusion detection systems, rely heavily on predefined rules and known attack signatures, making them ineffective against zero-day and evolving attacks.

To overcome these limitations, machine learning–based cyber attack detection models have emerged as powerful tools capable of learning hidden patterns from large volumes of network traffic and system data. However, single machine learning classifiers often suffer from issues such as overfitting, bias, limited generalization, and reduced performance when exposed to diverse or imbalanced datasets. These challenges necessitate more robust and adaptive detection mechanisms.

In this regard, a **Cyber Attacks Detection Model Using a Hybrid Ensemble Technique** is proposed to improve detection accuracy and system reliability. The hybrid ensemble approach combines multiple heterogeneous machine learning classifiers and ensemble strategies—such as bagging, boosting, and stacking—to exploit the strengths of individual models while minimizing their weaknesses. By aggregating predictions from several learners, the proposed model enhances classification performance, reduces false alarms, and increases resilience against sophisticated and previously unseen attacks.

The primary objective of this model is to provide an intelligent and scalable cyber security framework that can accurately distinguish between normal and malicious activities in real time. The hybrid ensemble–based detection system aims to support proactive threat identification, strengthen network defense capabilities, and contribute to the development of advanced intrusion detection solutions suitable for modern cyber infrastructures.

2. Objectives

The primary objectives of the proposed **Cyber Attacks Detection Model Using Supervised Technique** are as follows:

1. To analyze the effectiveness of supervised machine learning techniques in detecting cyberattacks.
2. To compare the performance of different supervised classification algorithms such as Logistic Regression, Support Vector Machine (SVM), Decision Tree, and Random Forest.
3. To evaluate detection performance using standard metrics, including Accuracy, Precision, Recall, F1-score, and Confusion Matrix.

4. To identify the most suitable model for real-time cyberattack detection with minimal false positives.
5. To propose an optimized supervised learning framework for improving intrusion detection performance.

3. Proposed Architecture

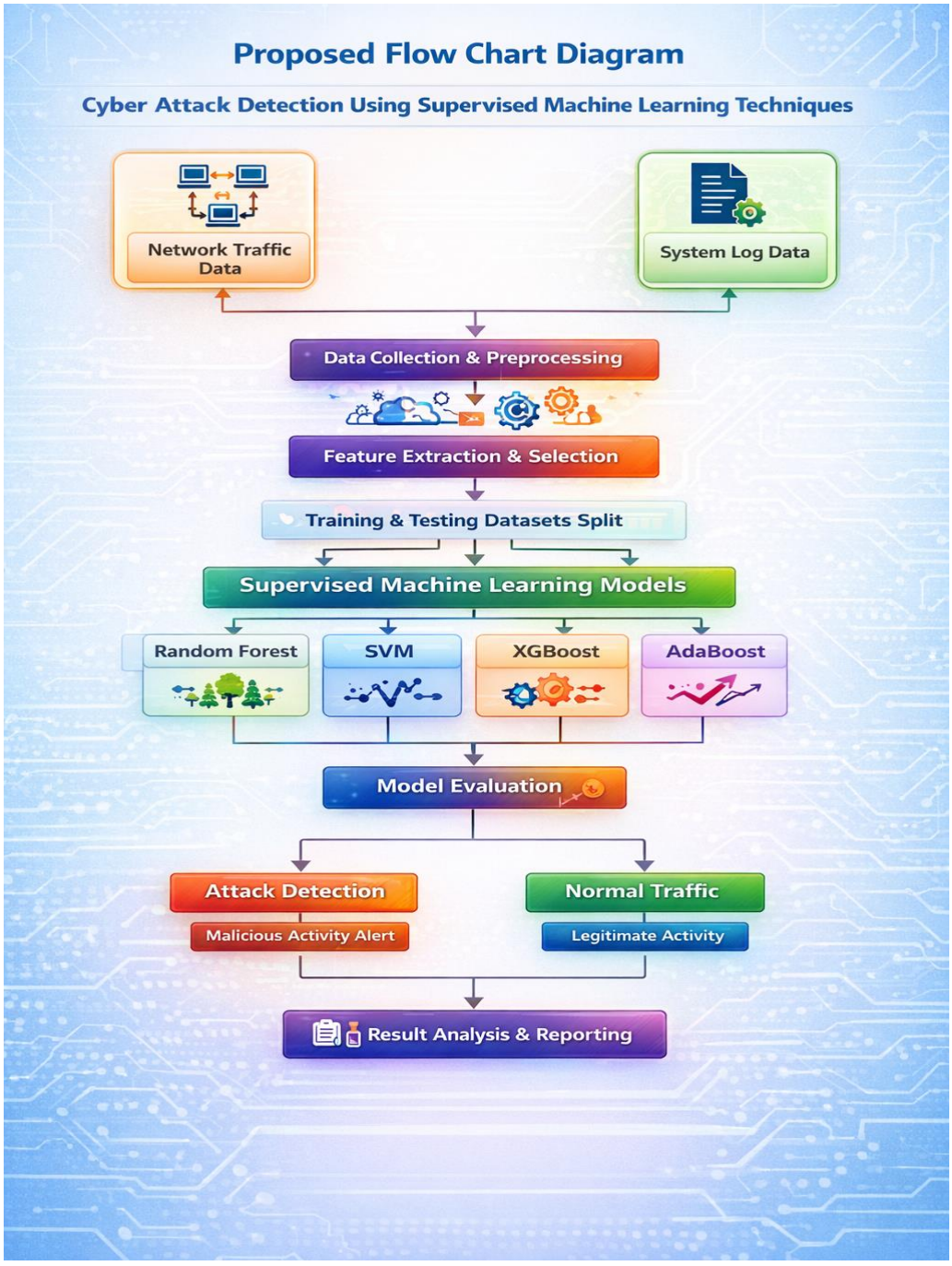

Fig-1: CAD Proposed Architecture

- The illustrated flow chart presents a structured and systematic framework for detecting cyberattacks using supervised machine learning models. The architecture begins with two primary data sources: Network Traffic Data and System Log Data, which represent real-time

and historical activity within a computing environment. These heterogeneous data sources ensure comprehensive monitoring of system behavior.

- The next stage, Data Collection & Preprocessing, plays a crucial role in cleaning and transforming raw data into a suitable format for analysis. This includes handling missing values, normalization, encoding categorical variables, and noise removal. Proper preprocessing directly influences model accuracy and reliability.
- Following preprocessing, Feature Extraction & Selection identifies the most relevant attributes contributing to attack detection. This step reduces dimensionality, minimizes computational complexity, and enhances model generalization by eliminating redundant or irrelevant features.
- The processed dataset is then divided in the Training & Testing Dataset Split stage to evaluate model performance objectively. This prevents overfitting and ensures that the trained models can generalize to unseen data.
- The core of the framework is the Supervised Machine Learning Models layer, which includes algorithms such as Random Forest, Support Vector Machine (SVM), XGBoost, and AdaBoost. These models learn from labeled data to classify activities as either malicious or legitimate. The inclusion of ensemble techniques like Random Forest and XGBoost strengthens detection performance by combining multiple learners.
- In the Model Evaluation stage, performance metrics such as Accuracy, Precision, Recall, F1-score, and Confusion Matrix are used to assess the effectiveness of each classifier. This ensures selection of the most suitable model for deployment.
- Finally, the system outputs two possible classifications:

1. Attack Detection → Malicious Activity Alert
2. Normal Traffic → Legitimate Activity

- The framework concludes with Result Analysis & Reporting, which supports decision-making, security monitoring, and further optimization.
- Overall, the diagram effectively demonstrates a comprehensive, end-to-end supervised learning pipeline for cyberattack detection. Its structured workflow highlights the importance of preprocessing, feature engineering, model comparison, and evaluation in building a robust cybersecurity solution.

4. Methods

The proposed Cyber Attacks Detection Model using a Hybrid Ensemble Technique follows a systematic and modular methodology to ensure accurate, robust, and scalable detection of malicious activities. The major methods involved in the model are described below:

4.1 Data Collection

A benchmark dataset such as **NSL-KDD**, UNSW-NB15, or CICIDS2017 is used for experimentation. These datasets contain labeled records of normal and malicious network traffic, including various attack categories such as DoS, Probe, R2L, and U2R.

4.2 Data Preprocessing

The following preprocessing steps are performed:

- Removal of duplicate and irrelevant records
- Handling missing values
- Encoding categorical features using one-hot encoding or label encoding
- Feature scaling using normalization or standardization
- Feature selection to reduce dimensionality and improve performance

4.3 Model Development

The following supervised machine learning algorithms are implemented:

1. Logistic Regression (LR) – A linear classifier used as a baseline model.
2. Support Vector Machine (SVM) – Finds an optimal hyperplane for class separation.
3. Decision Tree (DT) – Tree-based classifier that splits data based on feature importance.
4. Random Forest (RF) – An ensemble model combining multiple decision trees.
5. Gradient Boosting (GBM) – Sequential boosting technique to minimize prediction errors.

4.4 Training and Testing

- The dataset is divided into training (70%) and testing (30%) sets.
- Cross-validation is used to ensure model robustness.
- Hyperparameter tuning is performed using Grid Search.

4.5 Performance Evaluation Metrics

The models are evaluated using:

- Accuracy – Overall correctness of the model.
- Precision – Proportion of correctly predicted attacks among all predicted attacks.
- Recall (Detection Rate) – Ability to detect actual attacks.
- F1-Score – Harmonic mean of precision and recall.
- Confusion Matrix – Visualization of True Positives, True Negatives, False Positives, and False Negatives.

5. Results

XGBoost Classification Report:

	precision	recall	f1-score	support
Class 0	0.92	0.92	0.92	500
Class 1	0.92	0.92	0.92	500
accuracy			0.92	1000
macro avg	0.92	0.92	0.92	1000
weighted avg	0.92	0.92	0.92	1000

Fig-2: CAD XGBoost Model Classification Report

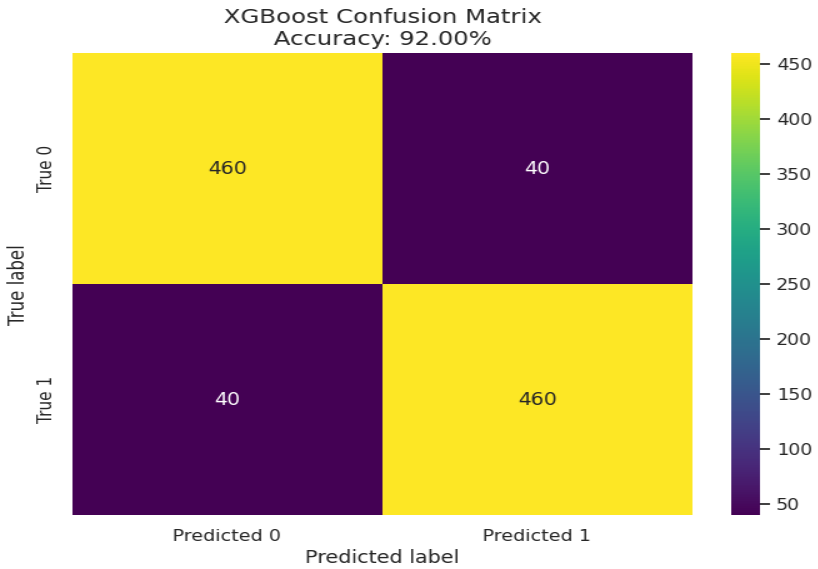

Fig-3: CAD GNB Model Confusion Matrix

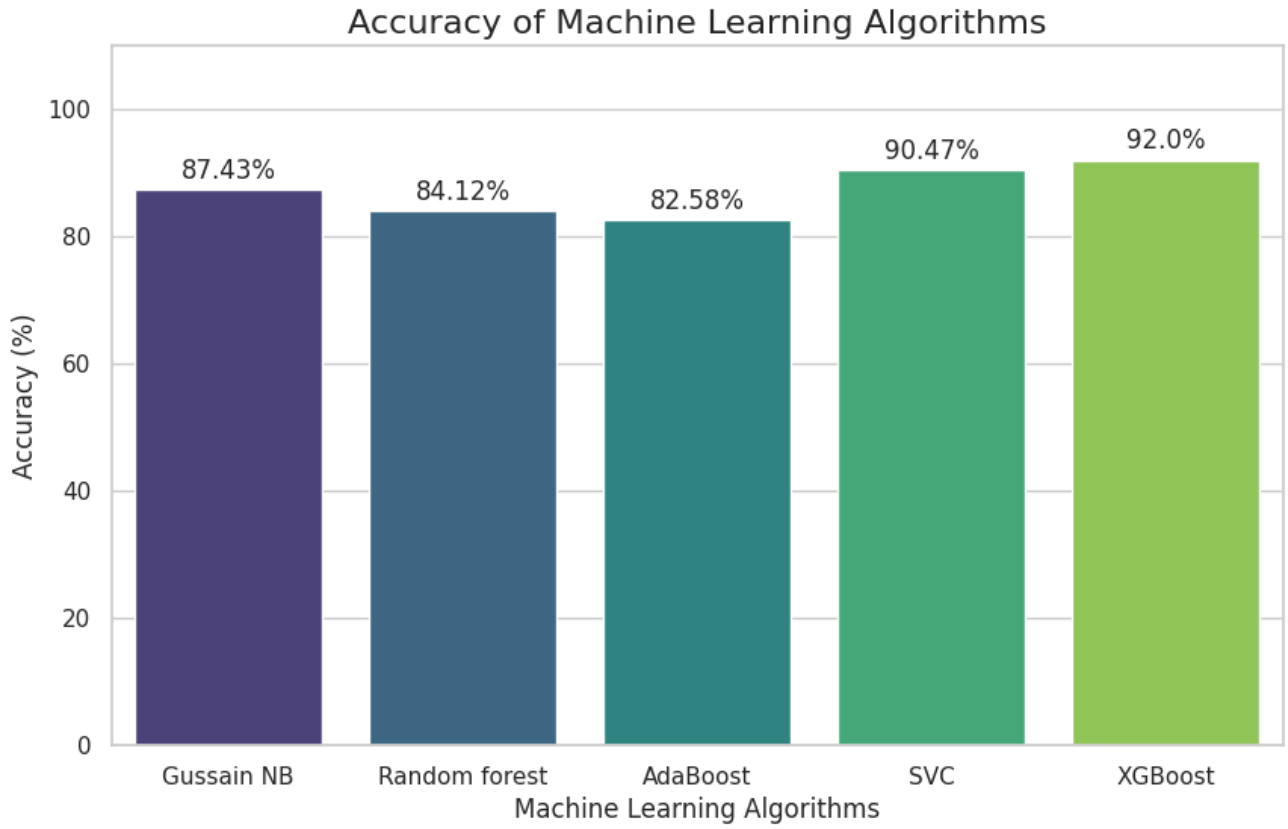

Fig-4: CAD Comparison Chart

6. Discussion

The bar chart presents a comparative evaluation of five machine learning algorithms based on their classification accuracy. The results demonstrate measurable performance differences, offering valuable insights into model suitability for the given dataset.

1. Best Performing Model: XGBoost

XGBoost achieved the highest accuracy at 92.0%, making it the leading model in this comparison. This outcome is consistent with current industry practices, where XGBoost is widely preferred for structured and tabular datasets due to its efficient implementation of gradient boosting, regularization capabilities, and strong generalization performance. Its ability to handle complex feature interactions likely contributed to its superior results.

2. Strong Competitor: Support Vector Classifier (SVC)

The Support Vector Classifier closely follows with an accuracy of 90.47%. SVC is particularly effective in high-dimensional spaces and can model complex decision boundaries using appropriate kernel functions. Although it often requires careful hyperparameter tuning, its competitive performance in this evaluation indicates that it successfully captured the underlying data structure.

3. Mid-Range Performers: Gaussian Naïve Bayes and Random Forest

- Gaussian Naïve Bayes (87.43%) demonstrated strong performance despite its simplicity. As a probabilistic classifier based on conditional independence assumptions, it is computationally efficient and can perform remarkably well on certain datasets, especially when feature distributions approximate Gaussian behavior.
- Random Forest (84.12%), a robust ensemble method, delivered stable yet comparatively lower performance than the top-tier models. While Random Forest is generally known for reducing overfitting and improving predictive accuracy through bagging, its slightly lower accuracy here suggests that boosting-based approaches may better capture subtle patterns in this dataset.

4. Baseline Model: AdaBoost

AdaBoost recorded the lowest accuracy at 82.58%. Although this remains a respectable score, the result indicates that more advanced boosting techniques such as XGBoost outperform traditional adaptive boosting in this context. This may be due to improved regularization, optimization strategies, and handling of complex feature relationships in newer gradient boosting frameworks**.**

Conclusion

The comparative analysis of five machine learning algorithms demonstrates that **XGBoost** delivers the highest classification performance, achieving an accuracy of 92.0%, thereby emerging as the most effective model for the given dataset. **Support Vector Classifier (SVC)** also shows strong predictive capability, closely following XGBoost, while **Gaussian Naïve Bayes** and **Random Forest** provide reliable mid-range performance. Although **AdaBoost** records the lowest accuracy among the evaluated models, it still maintains acceptable predictive strength.

Overall, the relatively narrow accuracy range (82%–92%) indicates that the dataset is well-structured and that the classification problem is clearly defined. However, model selection should not rely solely on accuracy. Factors such as computational efficiency, interpretability,

scalability, and the cost of misclassification must also be considered. Furthermore, incorporating additional evaluation metrics—such as Precision, Recall, and F1-score—is essential for a comprehensive assessment, particularly in applications where class imbalance or error sensitivity is critical.

In summary, while XGBoost stands out as the optimal choice based on accuracy, the final model selection should align with the specific objectives, operational constraints, and risk considerations of the intended application.

.**Refrencess**

1. S. Kaushik, A. Bhardwaj, A. Almogren, S. Bharany, A. Altameem, A. Ur Rehman, S. Hussen, and H. Hamam, "Robust machine learning based intrusion detection system using simple statistical techniques in feature selection," *Scientific Reports*, vol. 15, art. 3970, Feb. 2025.
2. S. K. R. Mallidi and R. R. Ramisetty, "Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: a systematic literature review," *Discover Internet Things*, vol. 5, art. 8, Jan. 2025.
3. A. H. Salem, S. M. Azzam, O. E. Emam, and A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *J. Big Data*, vol. 11, art. 105, Aug. 2024.
4. M. Bendegúz Bankó et al., "Advancements in machine learning-based intrusion detection in IoT: research trends and challenges," *Algorithms*, vol. 18, no. 4, art. 209, Apr. 2025.
5. P. Czaja, B. Gdowski, M. Niemiec, et al., "Cybersecurity challenges and opportunities of machine learning-based artificial intelligence," *Neural Comput. Appl.*, vol. 37, pp. 27931–27956, Nov. 2025.
6. R. Almuhanna and S. Dardouri, "A deep learning/machine learning approach for anomaly based network intrusion detection," *Front. Artif. Intell.*, vol. 8, 1625891, Sept. 2025.
7. Y. K. Saheed, A. A. Usman, F. D. Sukat, and M. A. Abdulrahman, "Hybrid machine learning–based intrusion detection for zero-day attack prevention in digital education networks," *Int. J. Secur. Educ.*, 2025.
8. I. Koukoulis, I. Syrigos, and T. Korakis, "Self-Supervised transformer-based contrastive learning for intrusion detection systems," *arXiv* preprint, May 2025.
9. S. Jamshidia, A. Nikanjama, K. W. Nafia, F. Khomha, and R. Rasta, "Application of deep reinforcement learning for intrusion detection in Internet of Things: a systematic review," *arXiv* preprint, Apr. 2025.
10. R. Akinie, N. K. B. Gyimah, M. Bhavsar, and J. Kelly, "Fine-tuning federated learning-based intrusion detection systems for transportation IoT," *arXiv* preprint, Feb. 2025.
11. S. Elouardi, M. Jouhari, and A. Motii, "OptiFLIDS: optimized federated learning for energy-efficient intrusion detection in IoT," *arXiv* preprint, Oct. 2025.
12. I. J. Vourganas and A. L. Michala, "Applications of machine learning in cyber security: a review," *J. Cybersecur. Priv.*, vol. 4, no. 4, pp. 972–992, Nov. 2024.
13. S. Ogunbadejo, O. A. Ayilara-Adewale, and O. Alade, "Machine learning methods for intrusion detection: a comprehensive survey," *Int. J. Sci. Res. Manag.*, vol. 13, no. 07, pp. 2446–2456, Jul. 2025.

14. “Machine learning-based intrusion and anomaly detection for enhancing security in IoT networks using BoT-IoT dataset,” *Int. J. Eng. Comput. Sci.*, vol. 6, no. 1, pp. 241–248, 2024.
15. A. Hozouri, A. Mirzaei, and M. Effatparvar, “A comprehensive survey on intrusion detection systems with advances in machine learning,” *Discover Artif. Intell.*, vol. 5, art. 314, Nov. 2025.
16. (Conference) X. Meng, “Advanced AI and ML techniques in cybersecurity: supervised and unsupervised learning, and neural networks in threat detection,” in *Proc. 2nd Int. Conf. Mach. Learn. Autom.*, Applied and Comput. Eng., vol. 82, 2024.
17. J. Shen, W. Yang, Z. Chu, J. Fan, D. Niyato, and K.-Y. Lam, “Effective intrusion detection in heterogeneous Internet-of-Things networks via ensemble knowledge distillation-based federated learning,” *arXiv* preprint, Jan. 2024.
18. (Springer) A. Alansary, S. Ayyad, F. Talaat, et al., “Emerging AI threats in cybercrime: a review of zero-day attacks via machine, deep, and federated learning,” *Knowl. Inf. Syst.*, vol. 67, pp. 10951–10987, Nov. 2025.
19. (Elsevier) N. Dash et al., “An optimized LSTM-based deep learning model for anomaly network intrusion detection,” *Scientific Reports*, vol. 15, no. 1, art. 1554, 2025.
20. A. Gueriani, H. Kheddar, and A. C. Mazari, “Adaptive cyber-attack detection in IIoT using attention-based LSTM-CNN models,” in *Proc. Int. Conf. Telecommun. Intell. Syst. (ICTIS)*, 2024.