A Review on Supervised Machine Learning Techniques for Enhancing Cyber Threat Prediction Accuracy

Bandana Gupta, Chandra Shekhar Gautam
AKS, University, Satna, MP, India

How to Cite this Article:

Gupta, B. & Gautam, C. S. (2026). A Review on Supervised Machine Learning Techniques for Enhancing Cyber Threat Prediction Accuracy. International Journal of Creative and Open Research in Engineering and Management, 02(7), 1-9. https://doi.org/10.55041/ijcope.v2i7.186

https://doi.org/10.55041/ijcope.v2i7.186

Abstract

The rapid expansion of digital infrastructures has increased the magnitude and sophistication of cyber threats, making timely and accurate threat prediction a foundational requirement for modern cyber-security systems. We use multiple algorithms—including Random Forest, Gradient Boosting Machines, and Deep Neural Networks—on benchmark intrusion-detection datasets and real-world enterprise log samples. Experimental results demonstrate that an ensemble-optimized model achieves improved predictive accuracy, reduced false positives, and enhanced generalization to unseen attack patterns. The study highlights important feature engineering techniques, model-optimization strategies, and deployment considerations for practical cyber-security environments. This research focuses on developing a supervised machine learning model to improve the accuracy of cyber threat prediction by leveraging historical and labeled cyber-security data.

Experimental analysis on a benchmark transaction dataset demonstrates that unsupervised models can achieve over 90% recall in detecting abnormal activities, providing a scalable and adaptive defense against evolving cyber threats in online banking.

Keywords: Cyber-security, Online Banking, Behavioral Analysis, Unsupervised Learning, Anomaly Detection, Fraud Detection

1. Introduction

The rapid expansion of digital technologies, cloud computing, and internet-based services has significantly transformed modern society, enabling seamless communication, data exchange, and financial transactions. However, this technological advancement has also led to a substantial rise in cyber threats; including malware attacks, phishing, ransom ware, and network intrusions. These threats have become increasingly sophisticated, dynamic, and difficult to detect, posing serious challenges to individuals, organizations, and governments worldwide. As cyber-attacks continue to evolve in complexity and scale, ensuring robust and proactive cyber-security mechanisms has become a critical priority [1].

Traditional cyber-security approaches, such as signature-based and rule-based detection systems, have been widely used to identify known threats. While effective against previously identified attack patterns, these methods struggle to detect zero-day attacks and emerging threats due to their reliance on predefined rules and static databases. Consequently, there is a growing need for intelligent systems capable of learning from data and adapting to new threat patterns in real time.

In this context, machine learning has emerged as a powerful tool in cyber-security, offering the ability to analyze large volumes of data, identify hidden patterns, and make accurate predictions. Among various machine learning paradigms, supervised learning techniques have gained particular attention due to their effectiveness in classification and prediction tasks using labeled datasets [5]. Algorithms such as Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines (SVM) have shown promising results in detecting and classifying cyber threats with improved accuracy.

Despite these advancements, several challenges remain in developing highly accurate cyber threat prediction models. Issues such as imbalanced datasets, irrelevant or redundant features, high false positive rates, and lack of real-time adaptability often limit the performance of existing models. Therefore, there is a need to design a robust supervised machine learning framework that addresses these challenges through effective data preprocessing, feature selection, and model optimization techniques.

2.Literature Review

The increasing frequency and sophistication of cyber threats have driven extensive research into the application of machine learning (ML) techniques for effective threat detection and prediction. Traditional security mechanisms, primarily based on signature and rule-based approaches, have been widely reported as insufficient for detecting emerging and unknown cyber-attacks. These limitations have motivated researchers to explore intelligent, data-driven approaches capable of identifying complex and evolving threat patterns.

Recent literature highlights that machine learning plays a critical role in modern cyber-security systems by enabling automated pattern recognition, anomaly detection, and predictive analytics. ML techniques can process large volumes of high-dimensional data and identify hidden relationships that are often undetectable through conventional methods [6]. As a result, ML-based models have become central to intrusion detection systems (IDS), malware detection, and network traffic analysis.

Comparative chart of Literature review

S.No	Author(s) & Year	Study Focus	Techniques Used (Supervised ML)	Dataset / Environment	Key Findings	Limitations
1	Vaka & Sharma (2023)	Review of ML in cyber threat detection	Decision Trees, SVM, Classification models	General cybersecurity datasets	ML improves detection of hidden attack patterns and enhances predictive capability	Lack of real-time implementation focus
2	Naseer (2022)	Intrusion Detection System (IDS) using ML	Supervised & Hybrid models	IDS network traffic data	Supervised learning improves IDS accuracy and reduces response time	Performance depends on feature selection
3	Doris & Shad (2024)	Cyber-attack prediction using ML algorithms	Decision Trees, SVM, Neural Networks	Network traffic datasets	High accuracy in predicting cyber-attacks; ML enables proactive defense	Data quality and imbalance issues
4	Kumar & Selvaraj (2025)	ML approaches for cyber threat detection	Classification algorithms (supervised models)	Large-scale cybersecurity datasets	Improved accuracy using feature selection and evaluation metrics (F1, precision)	Challenges in explain ability and privacy
5	Ambritha & Surendhiran	Hybrid ML framework	Random Forest,	IDS logs, malware	Ensemble + supervised	Computational complexity

	(2024)	for prediction & prevention	XGBoost, CNN, RNN	datasets	models significantly improve prediction accuracy and reduce false positives	
6	Tin et al. (2023)	Behavioral-based threat prediction	Logistic Regression, KNN, Decision Tree, SVM, Naïve Bayes	Behavioral user dataset	Supervised models effectively classify user behavior for threat prediction	Limited dataset size
7	Kok et al. (2020)	ML techniques for cyber threat prediction	Supervised + Deep Learning approaches	NATO simulation datasets	ML helps detect advanced persistent threats in complex environments	Requires high computational resources
8	Reddy (2023)	Cybersecurity threat prediction using ML	Supervised classification models	Network traffic and malware data	ML enables real-time detection and proactive mitigation	Difficulty handling zero-day attacks
9	Kravchuk & Korobeinikova (2024)	Evaluation of ML-based prediction models	Supervised learning & neural networks	Cybersecurity datasets	ML enhances detection capability and supports real-time systems	Requires large training data
10	Dalal et al. (2023)	IoT cyber-attack prediction	SVM, Decision Tree (supervised)	IoT network datasets	Multi-class SVM improves prediction accuracy in IoT environments	Scalability issues

A systematic review of studies published between 2016 and 2024 reveals that supervised machine learning algorithms are among the most widely used techniques for cyber threat detection. Algorithms such as Random Forest, Decision Trees, Support Vector Machines (SVM), and Naïve Bayes have demonstrated strong performance in classification tasks. Among these, Random Forest has been consistently identified as one of the most effective models due to its high accuracy and robustness across multiple datasets. Similarly, comparative studies show that supervised learning techniques models, achieving accuracy levels as high as 97–99% in intrusion detection tasks [7].

Several research works have focused on improving detection accuracy through feature engineering and model optimization. Feature selection techniques, such as correlation-based methods and dimensionality reduction, have been shown to enhance model performance by eliminating redundant and irrelevant attributes. Some studies report detection accuracy exceeding 98–99% when using deep and hybrid models, particularly in complex scenarios such as IOT

security and malware analysis. However, these models often require high computational resources and large datasets, limiting their practical deployment in real-time systems [10].

Despite significant progress, the literature identifies several challenges in the development of effective cyber threat prediction models. One major issue is the imbalance and lack of diversity in available datasets, which can lead to biased models and reduced generalization capability. Additionally, many existing datasets are outdated and fail to represent modern attack patterns, affecting the reliability of trained models. Other challenges include over fitting, high computational cost, lack of explain ability, and difficulty in handling real-time data streams.

Furthermore, recent studies emphasize the need for adaptive and scalable models capable of detecting zero-day attacks and evolving cyber threats. While supervised learning models perform well on labeled datasets, their dependency on historical data limits their ability to detect previously unseen attacks. This has led to the exploration of hybrid frameworks that combine supervised and unsupervised learning for improved detection capability.

In short, the existing body of research demonstrates that supervised machine learning techniques have significantly improved the accuracy of cyber threat detection compared to traditional approaches. However, limitations related to dataset quality, model adaptability, and real-time performance highlight the need for further research. Therefore, developing an optimized supervised machine learning model that addresses these challenges remains an important area of study in cyber-security.

3. Identified Research Gap

Despite the significant advancements in applying supervised machine learning techniques for cyber threat detection and prediction, several critical gaps remain in the existing body of research. These gaps limit the effectiveness, scalability, and real-world applicability of current models and highlight the need for further investigation.

One of the major gaps identified is the limited accuracy and generalization capability of existing models. Although many studies report high accuracy on benchmark datasets, these models often fail to perform consistently when applied to real-world environments. This is primarily due to over-fitting and the lack of diverse, up-to-date datasets that reflect modern and evolving cyber threat patterns [8].

Another important gap lies in the issue of imbalanced datasets. Most cyber-security datasets contain a disproportionately large number of normal instances compared to malicious ones. As cyber threats continuously evolve, there is a need for models that can adapt to new and unseen attack patterns efficiently. Complex models, especially ensemble and deep learning approaches, often act as “black boxes,” making it difficult for cyber-security professionals to understand the reasoning behind predictions and take informed decisions [4].

Finally, there is insufficient emphasis on integrating optimization techniques, such as hyper-parameter tuning and hybrid model design, to enhance overall performance. Many studies focus on single algorithms without exploring combinations or optimization strategies that could significantly improve detection accuracy.

Identified Research Gaps

(i) Limited real-world applicability and generalization
(ii) Imbalanced and outdated datasets
(iii) Inefficient feature selection methods
(iv) High false positive rates
(v) Lack of real-time and adaptive models
(vi) Poor model interpretability
(vii) Insufficient use of optimization and hybrid approaches

4. Research Methodology

The methodology is structured into multiple stages, including data collection, preprocessing, model development, evaluation, and validation.

Research Design

The study follows a quantitative and experimental research design, where supervised machine learning techniques are applied to labeled cyber-security datasets. The objective is to train models on historical data and evaluate their performance in predicting cyber threats accurately. The purpose is to critically analyze and synthesize existing research on supervised machine learning techniques used for cyber threat prediction. This approach enables identification of trends, strengths, weaknesses, and research gaps in the domain.

Data Collection: it’s a systematic process of gathering information, observations, or measurements to answer a research question, test a hypothesis, or evaluate outcomes.

5. Data Sources

The research utilizes publicly available benchmark datasets commonly used in cyber-security research, such as:

(i) NSL-KDD dataset

(ii) KDD Cup 99 dataset

(iii) CICIDS (Canadian Institute for Cyber-security Intrusion Detection System dataset)

Data Description

(i) Features: Network traffic attributes (e.g., protocol type, service, duration, packet size)

(ii) Labels: Normal or attack categories (e.g., DoS, Probe, R2L, U2R)

Data Preprocessing

Data preprocessing is essential to ensure data quality and improve model performance.

Data Cleaning

(i) Removal of duplicate records

(ii) Handling missing or null values

(iii) Eliminating noisy and inconsistent data

Data Transformation

(i) Encoding categorical variables (e.g., one-hot encoding)

(ii) Feature scaling (normalization/standardization)

6. Comparative Analysis

Cyber threat detection has become a critical component of modern cyber-security systems due to the increasing frequency and sophistication of attacks such as malware, phishing, and intrusion attempts. Supervised machine learning (ML) models play a significant role in identifying and predicting such threats by learning patterns from labeled datasets. This section presents a comparative analysis of widely used supervised ML models based on their performance, efficiency, and suitability for cyber threat detection.

Comparative Evaluation of Models

S.No.	Model	Accuracy	Training Time	Scalability	Interpretability	Suitability
1	Decision Tree	Moderate	Low	Moderate	High	Small datasets, simple threats
2	SVM	High	High	Low	Medium	Complex pattern detection
3	Random Forest	Very High	Medium	High	Medium	General-purpose threat detection
4	Logistic Regression	Moderate	Low	High	High	Binary classification tasks
5	KNN	Moderate	Low (training) / High (testing)	Low	Low	Pattern-based detection
6	Naïve Bayes	Moderate	Very Low	High	Medium	Large datasets, real-time detection
7	ANN	Very High	High	High	Low	Complex and large-scale threats

7. Challenges and Limitations

While supervised machine learning techniques have significantly improved cyber threat prediction accuracy, they face several critical challenges related to data, scalability, adaptability, and interpretability.

Handling imbalanced datasets (normal vs attack traffic)

Detecting zero-day attacks

Trade-off between accuracy and computational cost

Lack of explain ability in complex models

8. Future Research Directions

Future research in supervised machine learning for cyber threat prediction should focus on building adaptive, explainable, and scalable models capable of addressing real-world cyber-security challenges. By integrating advanced techniques such as deep learning, hybrid models, and real-time analytics, researchers can significantly enhance prediction accuracy and develop more resilient cyber-security systems.

Use of hybrid models combining supervised and unsupervised learning

Application of deep learning and transfer learning for better adaptability

Development of Explainable AI (XAI) techniques

Use of data augmentation and resampling techniques to address class imbalance

Adoption of online learning models for real-time threat detection

9. Conclusion

This research design provides a structured framework to systematically review and analyze supervised machine learning techniques in cyber threat prediction. It ensures a comprehensive and unbiased evaluation of existing work while identifying key areas for improvement and future research. The comparative analysis indicates that no single supervised ML model is universally optimal for cyber threat detection. While Random Forest and ANN provide superior accuracy, simpler models like Logistic Regression and Naïve Bayes are more efficient for real-time applications. Therefore, selecting an appropriate model depends on factors such as dataset size, computational resources, and the nature of cyber threats. Hybrid and ensemble approaches are increasingly recommended to achieve a balance between accuracy and efficiency.

While supervised machine learning techniques have significantly improved cyber threat prediction accuracy, they face several critical challenges related to data, scalability, adaptability, and interpretability. Addressing these limitations is essential for developing robust, efficient, and real-time cyber-security systems capable of handling modern and evolving threats.

10. References

1. Srinivasulu, A., Kim, T., & Chinthaginjala, R. (2025). Leveraging data analytics to revolutionize cyber-security with machine learning and deep learning. Scientific Reports, 15.
2. Ankalaki, S., Rajesh, A., Pallavi, M., & Hukkeri, G. S. (2025). Cyber-attack prediction: From traditional machine learning to generative artificial intelligence. IEEE Access.
3. Ahmed, Y., Azad, M. A., & Asyhari, T. (2024). Rapid forecasting of cyber events using machine learning-enabled features. Information, 15(1).
4. Vourganas, I. J., & Michala, A. L. (2024). Applications of machine learning in cyber security: A review Journal of Cyber-security and Privacy, 4(4), 972–992.
5. Almahmoud, A., et al. (2025). Forecasting cyber threats and pertinent mitigation technologies. Technological Forecasting and Social Change, 210.
6. Sri Ambritha, S. K. (2024). Advanced machine learning algorithm for cyber-attack prediction and prevention. International Journal of Intelligent Systems and Applications in Engineering.
7. (2024). Predicting and mitigating cyber threats through data mining and machine learning. Computer Communications, 228.
8. (2024). Applying AI and machine learning to enhance automated cyber-security and network threat identification. Procedia Computer Science.
9. Redhu, A., Choudhary, P., Srinivasan, K., & Das, T. K. (2024). Deep learning-powered malware detection in cyberspace: A contemporary review. Frontiers in Physics, 12.
10. Salman, A. M., & Al-Nuaimi, B. T. (2025). Enhancing cyber-security with machine learning: A hybrid approach for anomaly detection and threat prediction. Mesopotamian Journal of Cyber-Security.
11. Enhancing Cyber Security By Predicting Malwares Using Supervised Machine Learning Models, International Journal of Computing and Artificial Intelligence, 2021; 2(2): 55-62
12. Gautam, C. S., & Pandey, P. (2022). A review on genetic algorithm models for Hadoop MapReduce in big data. International Journal of Recent Scientific Research, 13(3E), 771–775. https://doi.org/10.24327/ijrsr.2022.1303.0166
13. Gautam, C. S., Soni, L. N., & Pandey, P. (2022). Clustering of big data using genetic algorithm in Hadoop MapReduce. European Chemical Bulletin, 12, 963–973.

14. Gautam, C. S., & Waoo, A. A. (2024). Genetic algorithm vs ant colony optimization for offloading in mobile augmented reality. ShodhKosh: Journal of Visual and Performing Arts, 5.
15. Gautam, C. S., & Pandey, P. (2023). Improving query optimization process in Hadoop MapReduce using ACO-genetic algorithm and HDFS MapReduce technique. International Journal of Current Engineering and Technology, 13(2). https://doi.org/10.14741/ijcet/v.13.2.8
16. Gautam, C. S., & Pandey, P. (2019). A review of big data environment, tools and challenges. Journal of Emerging Technologies and Innovative Research, 6, 569–575.
17. Chaudhari, S., Gautam, C. S., & Waoo, A. A. (2024). Enhancing heart disease prediction accuracy: A comparative study of machine learning models with ensemble method. JARIIE, 10, 4827–4833.
18. Kar, S. K., Pandey, A., & Gautam, C. S. (2025). A review of machine learning techniques for breast cancer prediction. International Journal of Current Engineering and Technology, 15(3).
19. Shrivastava, P., Gautam, C. S., & Kar, S. K. (2024). Assessing the performance of Cataract Net and other deep learning systems for automated cataract detection. ShodhKosh: Journal of Visual and Performing Arts, 5(5).
20. Shrivastava, P., & Gautam, C. S. (2025). A systematic review of digital twin and reinforcement learning applications in underground load-haul-dump (LHD) systems. The Indian Mining & Engineering Journal, 64(10–11), 39–48.
21. Patel, H. S., Gautam, C. S., & Waoo, A. A. (2025). AI-powered intrusion systems in cybersecurity and zero-day attack detection. International Journal of Scientific Research in Engineering and Management (IJSREM), 9(11). https://doi.org/10.55041/IJSREM54733
22. Shrivastava, R., & Gautam, C. S. (2026). An optimized hybrid classification approach for early detection of heart disease. International Journal of Computer Science Trends and Technology (IJCST), 14(1), 25–31.
23. Gautam, C. S., & Waoo, A. A. (2024). Genetic algorithm vs ant colony optimization for offloading in mobile augmented reality. ShodhKosh: Journal of Visual and Performing Arts, 5(5), 352–361. https://doi.org/10.29121/shodhkosh.v5.i5.2024.1886
24. R. Shrivastva, C. S. Gautam, And S. K. Kar, “Promoting A Website with The Help of Seo Using Ppc (Pay Per Click),” Shodhkosh: Journal of Visual and Performing Arts, Vol. 5, No. 5, Pp. 133–140, May 2024, Issn (Online): 2582-7472, Doi: 10.29121/Shodhkosh.V5. I5.2024.361.