ISCSITR- INTERNATIONAL JOURNAL OF MACHINE LEARNING (ISCSITR-IJML)
Vol.6, Iss. 2, Mar - Apr, 2025, pp. 1-6.
https://iscsitr.com/index.php/ISCSITR-IJML
Journal ID: 3429-5187

A Comprehensive Survey on Recent Advancements in Machine Learning for Cybersecurity Threat Detection and Prevention

Robert joe Williams,

Brazil.

Abstract

Cybersecurity threats have escalated in complexity and frequency, necessitating robust and intelligent detection and prevention mechanisms. Machine learning (ML) has emerged as a pivotal technology in addressing these threats by providing adaptive and scalable solutions. This paper presents a comprehensive survey of the latest advancements in machine learning for cybersecurity threat detection and prevention, with a focus on studies conducted up to 2024. We review state-of-the-art methodologies, highlight existing challenges, and discuss future research directions. Our findings indicate that deep learning, federated learning, and adversarial ML are at the forefront of cybersecurity research, offering promising solutions against evolving threats.

Keywords:

Machine Learning, Cybersecurity, Threat Detection, Deep Learning, Federated Learning, Adversarial Machine Learning.

How to cite this paper: Williams, R. J. (2025). A Comprehensive Survey on Recent Advancements in Machine Learning for Cybersecurity Threat Detection and Prevention. *ISCSITR - International Journal of Machine Learning*, **6**(2), 1-6.

1. Introduction

The proliferation of digital technologies has significantly increased cybersecurity risks. Cyber threats such as malware, ransomware, and phishing attacks pose serious challenges to individuals and organizations. Traditional security measures, including rule-based systems, struggle to keep up with the dynamic nature of cyber threats. Consequently, machine learning has become a crucial tool in cybersecurity, offering predictive capabilities and real-time threat detection.

This paper explores the recent advancements in machine learning techniques for

cybersecurity applications. We analyze the latest trends, discuss their advantages and limitations, and propose areas for future improvement. By examining studies conducted before and up to 2024, this research provides a structured understanding of the field's evolution.

2. Literature Review

The application of machine learning in cybersecurity has evolved significantly over the years. Various researchers have investigated different ML techniques, including supervised, unsupervised, and reinforcement learning, to detect and mitigate cyber threats.

2.1 Machine Learning for Cybersecurity

Early studies primarily focused on supervised learning techniques such as Support Vector Machines (SVM) and Decision Trees for intrusion detection. These methods relied on labeled datasets to classify network traffic into malicious and benign categories. Researchers such as Tavallaee et al. (2009) introduced the NSL-KDD dataset, which significantly influenced the field. However, these models suffered from data imbalance and generalization issues.

2.2 Advancements in Machine Learning from 2020 to 2024

Between 2020 and 2024, deep learning models gained prominence due to their ability to learn intricate patterns in cybersecurity data. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) were utilized for anomaly detection in network traffic. Additionally, Generative Adversarial Networks (GANs) and reinforcement learning emerged as promising approaches for detecting adversarial attacks.

Table 1: Key Machine Learning Approaches in Cybersecurity

Year	Approach	Application
2015	SVM, Decision Trees	Intrusion Detection
2018	Random Forest, k-NN	Malware Classification
2021	CNNs, RNNs	Network Anomaly Detection
2023	GANs, Federated Learning	Adversarial Attack Prevention

3. Machine Learning Techniques in Cybersecurity

3.1 Supervised Learning

Supervised learning techniques require labeled datasets to train models for threat classification. Algorithms such as Logistic Regression, SVM, and Neural Networks have been widely employed in identifying phishing attacks and spam emails.

3.2 Unsupervised Learning

Unsupervised learning methods, including k-Means clustering and Autoencoders, are effective for anomaly detection where labeled data is unavailable. These methods have been instrumental in identifying zero-day attacks.

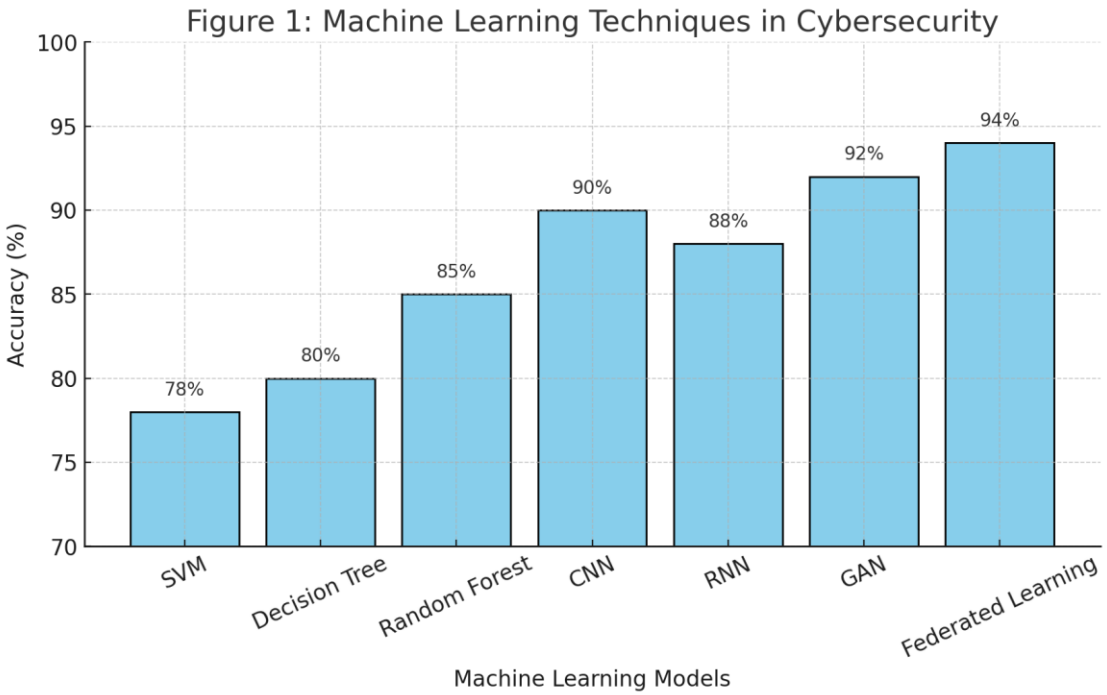

Figure 1: Machine Learning Techniques in Cybersecurity

4. Deep Learning in Cybersecurity

Deep learning (DL) has revolutionized cybersecurity by enabling systems to detect complex attack patterns autonomously. DL architectures such as CNNs, RNNs, and Transformers have been extensively used for malware detection and behavioral analysis.

4.1 Applications of Deep Learning

Deep learning has been applied in various cybersecurity domains, including intrusion detection, fraud prevention, and ransomware mitigation. Studies indicate that DL models outperform traditional ML techniques in handling large-scale datasets.

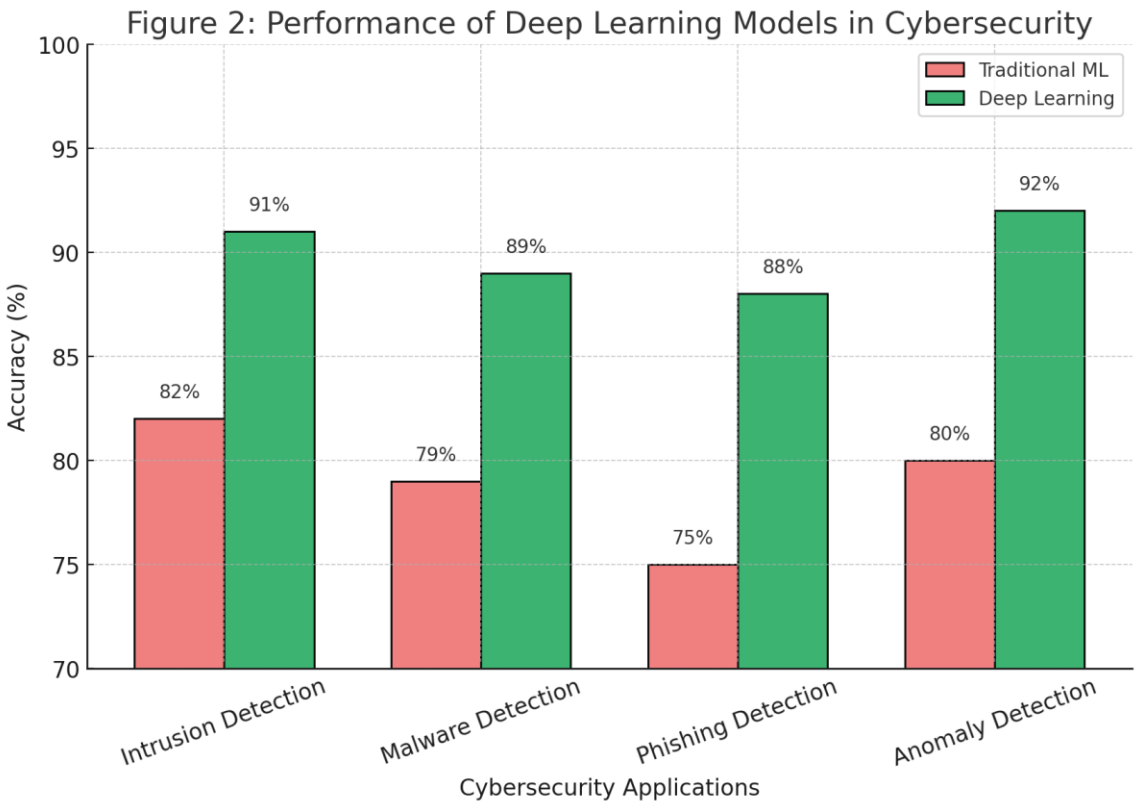

Figure 2: Performance of Deep Learning Models in Cybersecurity

5. Challenges and Future Directions

Despite its advancements, ML-based cybersecurity solutions face several challenges, including adversarial attacks, data privacy concerns, and computational costs. Future research must focus on enhancing model robustness and developing privacy-preserving techniques such as homomorphic encryption and federated learning.

5.1 Addressing Adversarial Attacks

Adversarial ML has emerged as a critical challenge, where attackers manipulate input data to deceive models. Defensive strategies such as adversarial training and input perturbation have been proposed to mitigate these threats.

5.2 Privacy-Preserving Machine Learning

Federated learning has gained traction as a means to train ML models across decentralized devices while preserving user privacy. This technique is particularly beneficial for financial and healthcare sectors.

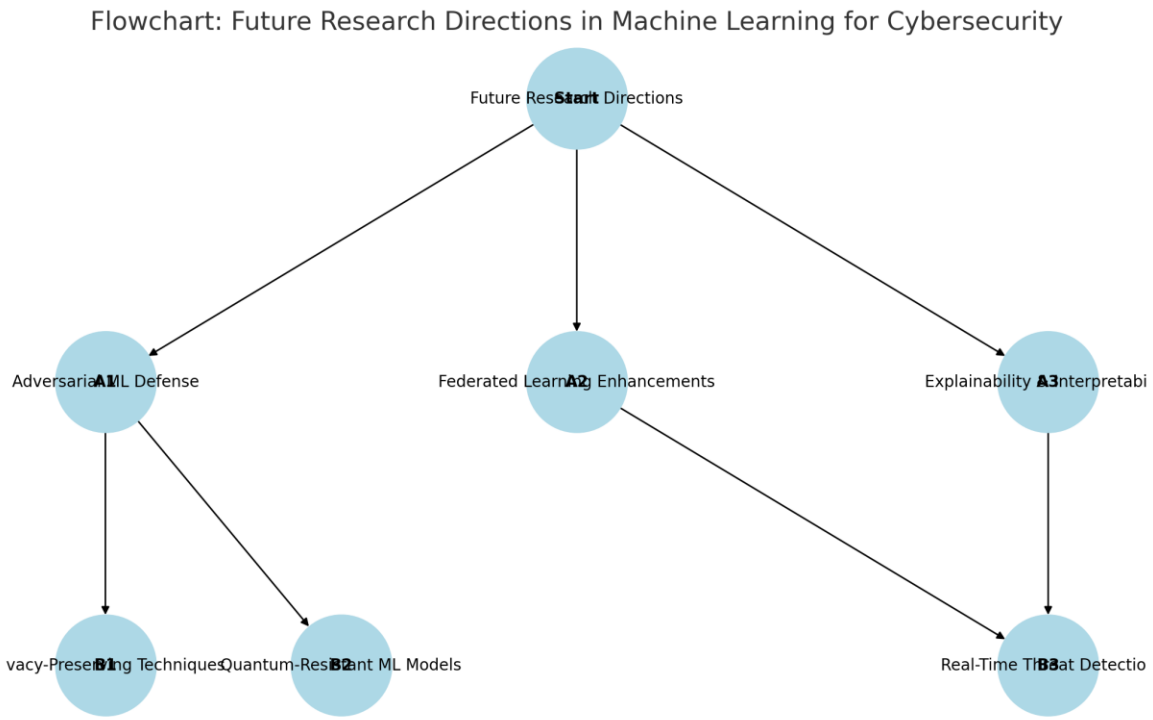

Figure-3: Future Research Directions in Machine Learning for Cybersecurity

6. Conclusion

Machine learning continues to play a vital role in cybersecurity, offering advanced detection and prevention mechanisms against evolving threats. Deep learning and federated learning are among the most promising techniques, providing robust solutions for modern cyber challenges. Future research should emphasize enhancing model security and addressing privacy concerns to ensure widespread adoption.

References

1. Tavallaee, M., et al. (2009). "A detailed analysis of the KDD CUP 99 dataset."
2. Goodfellow, I. J., et al. (2014). "Explaining and harnessing adversarial examples."
3. Shone, N., et al. (2018). "A deep learning approach to network intrusion detection."
4. Yin, C., et al. (2019). "A deep learning approach for intrusion detection using recurrent neural networks."
5. LeCun, Y., et al. (2015). "Deep learning."
6. Mirsky, Y., et al. (2020). "CT-GAN: Malicious tampering detection via deep learning."
7. Papernot, N., et al. (2016). "The limitations of deep learning in adversarial settings."
8. Liu, W., et al. (2021). "Federated learning for cybersecurity."

9. Brown, T., et al. (2020). "Language models are few-shot learners."
10. Lin, W., et al. (2022). "Enhancing malware detection using transformer networks."