Innovation and Integrative Research Center Journal

ISSN: 2584-1491 | www.iircj.org

Volume-2 | Issue-8 | August-2024 | Page 32-44

Machine Learning Algorithms for Predictive Cybersecurity

Vimlesh Sahu

Lecturer (JBS) Computer Science

Dr. Bhanwar Singh Porte Govt. P.G. College Pendra, G.P.M. Chhattisgarh

vims24sahu@gmail.com

Abstract

The increasing sophistication of cyber threats has necessitated the development of proactive cybersecurity strategies that can detect and prevent attacks before they cause harm. Machine learning (ML) has emerged as a powerful tool in predictive cybersecurity, capable of identifying patterns, anomalies, and potential threats with unprecedented accuracy. This paper provides a comprehensive review of various machine learning algorithms—supervised, unsupervised, semi-supervised, deep learning, and reinforcement learning—and their applications in predictive cybersecurity. Key areas of focus include intrusion detection, malware classification, phishing detection, and anomaly detection in network traffic. Through a comparative analysis, we evaluate the strengths, limitations, and computational requirements of each algorithm to determine their suitability for specific cybersecurity tasks. Additionally, we discuss the challenges facing ML in cybersecurity, such as data scarcity, computational demands, adversarial attacks, and privacy concerns. Finally, the paper explores future directions, including hybrid approaches, federated learning, and adaptive models, to address these challenges and enhance the effectiveness of ML in predictive cybersecurity. This review aims to provide researchers and practitioners with insights into the current state and future potential of machine learning for creating a more secure digital environment

Keywords: Predictive Cybersecurity, Machine Learning Algorithms, Intrusion Detection, Threat Detection, Anomaly Detection.

Introduction

With the exponential rise in cyber threats, from malware and phishing attacks to complex network intrusions, the need for proactive cybersecurity measures has become increasingly critical. Traditional, rule-based cybersecurity systems are limited in their capacity to anticipate and respond to emerging threats, as they primarily react to known vulnerabilities rather than predict new ones. This reactive approach leaves significant gaps in defenses, especially as cybercriminals employ more sophisticated tactics to bypass standard security protocols.

In recent years, machine learning (ML) has shown significant potential in transforming cybersecurity by enabling predictive capabilities. Machine learning algorithms can analyze vast datasets, identify patterns, and detect anomalies, empowering cybersecurity systems to detect threats at early stages and respond to them in near real-time. The predictive power of ML offers a promising approach to cybersecurity, providing organizations with the tools to anticipate, analyze, and mitigate risks before they escalate. This paper investigates the role of various machine learning algorithms in predictive cybersecurity, focusing on applications such as intrusion detection, malware classification, phishing prevention, and anomaly detection in network traffic. We provide a detailed analysis of different ML techniques—including supervised, unsupervised, semi-supervised, deep learning, and reinforcement learning—and assess their strengths, limitations, and applicability across diverse cybersecurity tasks. Furthermore, we explore the challenges of implementing ML in cybersecurity, including data quality issues, high computational requirements, susceptibility to adversarial attacks, and ethical concerns related to privacy.

The objective of this study is to guide researchers and practitioners in understanding the capabilities and limitations of current machine learning techniques in cybersecurity. By examining recent advancements, identifying existing gaps, and proposing future directions, this paper seeks to advance the field of predictive cybersecurity and contribute to the development of more resilient defenses against evolving cyber threats.

Literature Review

Machine learning has increasingly become a focus in the field of cybersecurity, aiming to enhance the predictive and responsive capabilities of security systems. Numerous studies have explored the potential of different machine learning algorithms in various cybersecurity applications, such as intrusion detection, malware analysis, phishing detection, and network anomaly detection. This literature review provides an overview of these studies and highlights the strengths, challenges, and advancements in the application of machine learning algorithms for predictive cybersecurity.

1. Evolution of Machine Learning in Cybersecurity

Historically, cybersecurity measures relied on rule-based systems that operated by identifying signatures of known threats. However, this approach had significant limitations in detecting new or unknown attacks, often referred to as "zero-day" attacks. The shift towards machine learning has enabled a more dynamic approach, where systems learn from vast data and adapt to evolving threats. Research by Sommer and Paxson [1] emphasized that traditional detection methods struggle with zero-day vulnerabilities, advocating for a data-driven approach where patterns of cyber behavior are learned over time. Similarly, Buczak and Guven [2] highlighted the value of anomaly detection models in spotting unusual network activities that may signify an attack.

2. Supervised Learning for Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are essential components of cybersecurity infrastructure, and supervised learning techniques have been extensively studied in this area. Studies demonstrate that algorithms such as Decision Trees, Support Vector Machines (SVM), and Naïve Bayes classifiers are effective in identifying malicious activities when trained on labeled datasets [3]. For example, a study by Patel et al. [4] utilized Random Forests and SVM for network intrusion detection and achieved high accuracy, demonstrating the effectiveness of supervised methods for IDS. However, the requirement of labeled data for supervised learning presents a significant challenge, as labeling cyberattack data can be time-consuming and costly.

3. Unsupervised Learning and Anomaly Detection

In contrast to supervised methods, unsupervised learning algorithms can detect anomalies without labeled data, making them highly suitable for unknown or evolving threats. Clustering techniques, such as K-Means and DBSCAN, are widely used for identifying outliers in network traffic, which often correlate with suspicious or malicious behavior [5]. Zhang et al. [6] showed that unsupervised models, like DBSCAN, could effectively detect anomalies in network traffic data, helping to identify potential threats that traditional systems might miss. However, as noted by Chandola et al. [7], unsupervised models often suffer from high false-positive rates, necessitating further refinement in practical applications.

4. Deep Learning for Advanced Threat Detection

Deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have gained traction in cybersecurity due to their ability to analyze complex patterns and large datasets. RNNs, particularly Long Short-Term Memory (LSTM) networks, have been effective in detecting time-sequence anomalies in network traffic, which are crucial for identifying ongoing threats in real-time [8]. Alom et al. [9] demonstrated that CNNs could achieve high accuracy in malware detection by analyzing malware signatures and patterns, thus providing a robust defense against polymorphic malware. However, these models are computationally intensive and require significant resources, which can limit their applicability in real-time cybersecurity environments [10].

5. Reinforcement Learning for Autonomous Threat Response

Reinforcement learning (RL) is another area of interest in predictive cybersecurity, particularly for its potential in autonomous threat response. Unlike supervised and unsupervised learning, RL models learn optimal actions through trial and error, making them suitable for applications like autonomous network defense. Research by Nguyen et al. [11] applied reinforcement learning to dynamic network protection, demonstrating its potential in making real-time decisions to mitigate attacks. However, RL models require extensive training and suffer from scalability issues, as noted by Shen et al. [12].

6. Challenges in Applying Machine Learning to Cybersecurity

The application of machine learning in cybersecurity faces several challenges, including data quality, computational demands, and adversarial attacks. High-quality data is critical for training accurate models, yet cybersecurity data is often incomplete or noisy, which can impact model performance. Buczak and Guven [2] pointed out the issue of limited labeled data, which affects the accuracy of supervised learning models in particular. Additionally, adversarial attacks pose a unique challenge, as cybercriminals attempt to deceive ML models by introducing subtle perturbations to data. Studies like that of Biggio et al. [13] explore adversarial ML, indicating the need for more robust models that can withstand such attacks.

7. Ethical and Privacy Concerns

Ethical and privacy issues also complicate the deployment of ML in cybersecurity. While predictive models can significantly improve threat detection, they often require access to sensitive data. Privacy-preserving ML techniques, such as federated learning, have been proposed as solutions, allowing models to learn from data distributed across multiple organizations without sharing sensitive information [14]. McMahan et al. [15] introduced federated learning as a method that preserves privacy while enabling predictive cybersecurity at scale.

Machine Learning Algorithms in Predictive Cybersecurity

Machine learning (ML) algorithms play a transformative role in predictive cybersecurity, enabling proactive detection and mitigation of threats across various domains, such as network security, malware detection, intrusion detection, and fraud prevention. By leveraging data-driven insights, ML algorithms help identify emerging threats, detect unusual patterns, and automate responses to cyber incidents. This section explores the most prominent ML algorithms utilized in predictive cybersecurity, focusing on their applications, advantages, and challenges.

1. Supervised Learning Algorithms

Supervised learning algorithms are widely used in cybersecurity for tasks where labeled data is available, such as classifying malware types or detecting known attack patterns. Key supervised learning algorithms include:

- **Support Vector Machines (SVM):** SVMs are effective in classifying large amounts of data and are often applied in intrusion detection systems (IDS) to differentiate between normal and malicious network activities. Research has shown SVM's ability to maintain high accuracy in identifying known threats, though its performance may degrade with evolving attack patternscision Trees and Random Forests:** Decision trees and ensemble methods, like random forests, are frequently used for classifying threats based on features in the data. For instance, random forests can analyze network traffic patterns to detect anomalies with high precision, leveraging the decision-making power of multiple tree models .

- **N:** Naïve Bayes classifiers, based on probabilistic methods, are popular in spam detection and email filtering. They calculate the likelihood of an email being malicious based on historical data, making them effective for handling simple classifications .

However, superning requires labeled datasets, which may not always be readily available, making it challenging to keep up with rapidly evolving threats.

2. Unsupervised Learning Algorithms

Unsupervised learning algorithms do not rely on labeled data, making them ideal for detecting unknown threats and identifying unusual behaviors in network traffic. Commonly used unsupervised algorithms in cybersecurity include:

- **K-Means Clustering:** K-Means clustering groups data points based on similarities and is commonly used in anomaly detection. By clustering network traffic data, K-Means can identify outliers that may indicate suspicious activities .
- **Principal Component(PCA):** PCA is used for dimensionality reduction, helping to simplify complex data while preserving essential features. PCA-based anomaly detection models can analyze large datasets, reducing the complexity of identifying malicious patterns .
- **Autoencoders:** Autoencoders network variant, are often applied to detect anomalies in cybersecurity. By learning data patterns during the training phase, they can detect unusual activities during the testing phase. Autoencoders are particularly effective for detecting deviations in network traffic that may signal potential attacks .

Unsupervised methods, however, can suffer false-positive rates, as the absence of labels can make it difficult to fine-tune models to specific threat scenarios.

3. Semi-Supervised Learning Algorithms

Semi-supervised learning combines both labeled and unlabeled data, allowing for the detection of both known and unknown threats. This approach is particularly useful in scenarios where only a portion of the data is labeled, as is often the case in cybersecurity.

- **Self-Training Models:** Self-training models can iteratively label the unlabeled data based on predictions, refining the model's ability to detect anomalies. This is effective in phishing detection, where initially labeled samples help the model generalize to other types of phishing emails .
- **Label Propagation:** This algorithm propagatesom labeled to unlabeled data within a graph structure, making it useful for detecting botnets or compromised nodes in a network. Label propagation enables the expansion of labeled datasets, helping to improve detection accuracy with minimal labeled data .

Semi-supervised methods provide a balance between supervisepervised techniques, offering flexibility in scenarios where labeled data is scarce.

4. Deep Learning Algorithms

Deep learning has shown significant potential in predictive cybersecurity due to its ability to learn complex representations of data, making it particularly useful in areas like malware detection, intrusion detection, and real-time threat detection.

- **Convolutional Neural Networks (CNNs):** CNNs are widely used in image recognition but are also effective in cybersecurity for detecting malware. By representing malware as binary images, CNNs can analyze patterns within the code structure, helping to identify malicious software with high accuracy .
- **Recurrent Neural Networks (RNNs) and LSTM:** RNNs and Long Shortry (LSTM) networks are particularly suited for analyzing sequences, making them effective in network intrusion detection where the model learns to detect temporal anomalies in network traffic .
- **Generative Adversarial Networks (GANs):** GANs have emerged as a useful tersarial training, where one network generates potential threats while the other tries to detect them. This can help create robust models that are better equipped to handle adversarial attacks .

Although deep learning models are powerful, they are computationally intensive, making pplication challenging. Additionally, deep learning models are often seen as "black boxes," which limits interpretability in cybersecurity applications where transparency is critical.

5. Reinforcement Learning (RL) Algorithms

Reinforcement learning (RL) algorithms are used in scenarios requiring continuous learning and decision-making. RL models learn by interacting with the environment, making them suitable for real-time threat detection and autonomous cybersecurity responses.

- **Q-Learning:** Q-Learning is a model-free RL algorithm where the agent learns a policy for action based on rewards. It is effective in network defense systems, where it can learn strategies to respond to attacks dynamically .
- **Deep Q-Networks (DQN):** DQN combines deep learning with Q-learning, enhancing its ability toex decisions. It has been applied to create intelligent firewalls and adaptive network defense systems that can learn from attack patterns and respond accordingly .

Applications of Machine Learning in Predictive Cybersecurity

Machine learning (ML) has a broad range of applications in predictive cybersecurity, where it enables early detection, fast response, and proactive defense against sophisticated threats. Here are some critical areas where ML is being applied to enhance predictive cybersecurity:

1. Intrusion Detection and Prevention Systems (IDPS)

Machine learning algorithms are used to analyze vast amounts of network traffic data to identify malicious activity and prevent intrusions. By learning patterns of normal and abnormal behavior, ML models can detect unauthorized access, malware activity, and other suspicious behaviors. Some applications in this domain include:

- **Anomaly Detection:** ML-based anomaly detection algorithms such as Support Vector Machines (SVM), k-means clustering, and neural networks can identify unusual patterns in network traffic that may signify an attack.
- **Signature-based Detection:** Supervised learning models can be trained on labeled data to recognize known attack signatures, enabling quick identification of common threats like DoS and DDoS attacks **Malware Detection and Classification**

Malware detection is critical in cybersecurity, and machine learning has proven to be highly effective in distinguishing between benign and malicious files:

- **Static Analysis:** Machine learning models analyze characteristics of code or files without executing them to detect malware. Algorithms like decision trees, random forests, and neural networks can classify files based on features such as opcode sequences, control flow graphs, and API calls .
- **Dyysis:** In dynamic analysis, ML models analyze files in a controlled environment to observe their behavior. Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) models are especially useful here, as they can process the temporal sequences of system calls and detect patterns associated with malware behavior .

3. Phishion

Phishing attacks remain one of the most common cybersecurity threats, targeting individuals and organizations to steal sensitive information. ML models can analyze multiple features, such as email metadata, text content, and URL structures, to identify phishing attempts:

- **Natural Language Processing (NLP):** Using NLP techniques, ML models can detect anomalies in the language and content of emails, analyzing word patterns and structures commonly found in phishing messages.
- **URL Classification:** Algorithms such as Logistic Regression, Decision Trees, and Deep Learning models can classify URLs as legitimate or malicious based on characteristics like domain name, path, and HTML content .

4. User Behavior (UBA)

User behavior analytics (UBA) applies ML to monitor and analyze users' behavior patterns, which can help identify insider threats or compromised accounts:

- **Anomaly Detection Models:** Unsupervised ML techniques such as clustering and PCA (Principal Component Analysis) can track deviations from established behavior profiles, alerting security teams to unusual activities like large data transfers, unusual access times, or sudden changes in browsing behavior .
- **Predictive Modeling:** Predics can identify indicators of potential insider threats by analyzing a combination of factors, including access frequency, login patterns, and activity logs, helping organizations proactively respond to insider risks.

5. Fraud Detection

In areas such as finance and e-commerce, fraud detection is essential to prevent unauthorized transactions and financial loss. ML algorithms help detect fraudulent activities by analyzing transaction data in real time:

- **Anomaly and Outlier Detection:** Models such as SVM, Isolation Forests, and Autoencoders can flag outliers in transactional data that may indicate fraudulent transactions based on the deviation from normal spending behavior.
- **Supervised Learning for Known Frauds:** ML algorithms like Decision Trees and Neural Networks are trained on historical transaction data to learn patterns associated with fraud, allowing them to classify real-time transactions as legitimate or suspicious .

6. Network Traffic Analysis

Netwc analysis involves monitoring data flow across a network to detect potential threats and vulnerabilities. Machine learning is widely used to automate this analysis:

- **Botnet Detection:** ML models such as k-means clustering and neural networks can detect botnets by identifying unusual patterns in traffic behavior, such as coordinated activities or repetitive commands from infected machines.
- **Real-time Monitoring and Alerts:** By continuously analyzing network traffic, ML-based systems can provide real-time alerts for unusual or malicious activity, improving response times for security teams .

7. Threat Intelligence and Analysis

Machig algorithms support threat intelligence platforms that collect and analyze data from multiple sources, providing organizations with insights into emerging threats and attack trends:

- **Predictive Threat Modeling:** ML can forecast potential threats by analyzing current and historical attack data, which helps organizations prepare for and mitigate future attacks.
- **Data Correlation and Pattern Recognition:** Algorithms can correlate data from diverse sources, including social media, dark web, and threat feeds, to identify patterns that might indicate the early stages of an attack .

8. Spam and Anomaly Filtering

Spam filtering is onost common applications of machine learning in cybersecurity. ML models can distinguish between legitimate and spam content with high accuracy:

- **Email Spam Filtering:** Naïve Bayes, SVM, and neural networks are effective in filtering spam emails by analyzing the text, sender information, and embedded links.
- **Anomaly Filtering in Web Requests:** By analyzing HTTP request patterns, ML models can detect anomalies in web traffic, potentially blocking malicious web requests that could lead to attacks like SQL injections or Cross-Site Scripting (XSS) .

Comparative Analysis of Machine Learning Algorithms

Comparative analysis of common machine learning algorithms used in predictive cybersecurity, summarized in table format for clarity. This table compares each algorithm across various criteria such as typical use cases, strengths, weaknesses, accuracy, and computational complexity.

Algorithm	Typical Use Cases	Strengths	Weaknesses	Accuracy	Computational Complexity
Support Vector Machine (SVM)	Anomaly Detection, Intrusion Detection	Effective with high-dimensional data; good accuracy for binary classification tasks	Inefficient for large datasets; sensitive to noise	High for binary classification	$O(n^2)$ to $O(n^3)$ for training on large datasets
Decision Tree	Malware Detection, Phishing Detection	Interpretable; handles both categorical and continuous data	Prone to overfitting; can create complex trees	Moderate to High, depending on pruning	O(n * log(n)) for training
Random Forest	Malware Detection, Fraud Detection	Robust to overfitting; handles large datasets well; high accuracy	Slower in real-time applications; less interpretable	High	O(t * n * log(n)) where t = number of trees
K-Nearest Neighbors (KNN)	Intrusion Detection,	Simple to implement; good for	High memory usage; slower	Moderate	O(n) for prediction

	Anomaly Detection	smaller datasets	with large datasets		
Naïve Bayes	Spam Filtering, Phishing Detection	Fast and efficient with large datasets; interpretable results	Assumes feature independence; less accurate with correlated data	Moderate to High	O(n) for training and prediction
Neural Networks (Deep Learning)	Malware Detection, Dynamic Analysis	High accuracy with large datasets; good for complex patterns	Requires large datasets; computationally intensive	High, especially with deep models	O(n * m) per layer, where m = number of layers
Logistic Regression	Binary Classification (Spam, Phishing)	Interpretable; works well with linearly separable data	Limited to binary classification; less effective with complex patterns	Moderate	O(n) for training
K-Means Clustering	Anomaly Detection, Botnet Detection	Simple and efficient for clustering; scalable to large datasets	Sensitive to initial centroids; limited to spherical clusters	Moderate	O(n * k * t) where k = clusters, t = iterations
Recurrent Neural Network (RNN)	Dynamic Malware Detection, Behavior Analysis	Good for sequential data (e.g., system calls)	High computational cost; sensitive to vanishing gradient	High for sequence data	O(n * m) per time step, where m = number of layers
Isolation Forest	Anomaly Detection, Insider Threats	Effective for high-dimensional anomaly detection; low memory usage	Limited interpretability; sensitive to contamination level	Moderate to High	O(n * log(n))

Important Points:

- **Accuracy** varies significantly based on the dataset and task. Deep learning and ensemble methods like Random Forest tend to have high accuracy for complex tasks but are computationally demanding.
- **Computational Complexity** is essential for real-time applications; Naïve Bayes, KNN, and Logistic Regression are efficient for smaller datasets, while deep learning models require substantial computational resources.
- **Use Cases** indicate the flexibility of these algorithms across different cybersecurity tasks. Neural networks and Random Forests are versatile, while simpler models like Naïve Bayes are effective in well-defined contexts like spam filtering.

Future Directions

The application of machine learning in predictive cybersecurity is rapidly advancing, but significant opportunities remain to enhance both the efficacy and resilience of these systems. Key future directions include:

1. **Advanced Deep Learning Models**
   The use of deep learning models, including convolutional neural networks (CNNs) and generative adversarial networks (GANs), is expected to grow in predictive cybersecurity. These models can improve the detection of sophisticated threats, including evolving malware and advanced persistent threats (APTs). Research should focus on optimizing these models to balance detection accuracy with computational efficiency, especially for real-time applications.
2. **Federated Learning for Privacy-Preserving Security**
   Federated learning allows multiple organizations to collaboratively train models without sharing sensitive data, offering enhanced privacy and data security. Future work should explore federated approaches in cybersecurity, enabling threat intelligence sharing across institutions while respecting data privacy regulations like GDPR. This approach could help create robust models that benefit from diverse, decentralized datasets.
3. **Explainable AI (XAI) in Cybersecurity**
   With machine learning models increasingly used to automate critical security decisions, transparency and interpretability are paramount. Research in Explainable AI (XAI) aims to make these "black-box" models understandable to human analysts, helping them trust and act on machine-generated insights. Future work should prioritize developing interpretable models that allow security professionals to validate and explain model predictions, particularly for high-stakes decisions.
4. **Integration of Threat Intelligence**
   Integrating external threat intelligence feeds, including indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) used by cyber adversaries, can enhance the predictive accuracy of machine learning models. Future research should focus on fusing threat intelligence with machine learning to create adaptive models capable of responding to newly emerging threats in real time.
5. **Adversarial Machine Learning Defense Mechanisms**
   As machine learning models are increasingly targeted by adversarial attacks, there is a growing need for robust defenses. Future work should investigate the development of adversarial training methods and defensive algorithms that can enhance model resilience against evasion, poisoning, and model inversion attacks. Techniques like robust model architectures, anomaly detection layers, and retraining based on adversarial samples are promising areas for exploration.
6. **Real-Time Processing and Edge Computing**
   With the rise of IoT devices and the need for real-time security measures, deploying

machine learning models at the edge (near the data source) is becoming essential. Edge computing can reduce latency, enhance privacy, and enable rapid response in distributed environments. Future research should explore lightweight, resource-efficient models for edge-based predictive cybersecurity, especially for critical infrastructure and IoT deployments.

7. **Hybrid and Ensemble Approaches**
   Combining multiple algorithms, either through ensemble methods (e.g., Random Forests) or hybrid models (e.g., integrating supervised and unsupervised learning), can provide more accurate and comprehensive threat detection. Future studies should evaluate the effectiveness of hybrid approaches in addressing diverse cybersecurity threats, as well as the impact on interpretability, performance, and resource requirements.
8. **Adaptive Models with Reinforcement Learning**
   Reinforcement learning has potential applications in adaptive cybersecurity, where models learn optimal defense strategies through continuous interaction with a dynamic environment. Future research could develop reinforcement learning models that adaptively respond to new threats, automating tasks like intrusion response, access control, and anomaly mitigation.

Conclusion

The future of machine learning in predictive cybersecurity is promising, with emerging technologies and methodologies offering new capabilities to combat evolving cyber threats. By advancing research in areas such as deep learning, federated learning, XAI, adversarial defenses, and edge computing, the cybersecurity community can enhance the accuracy, efficiency, and resilience of predictive systems. Addressing these future directions will be essential in building adaptive, secure, and ethical machine learning models capable of safeguarding digital ecosystems against increasingly sophisticated cyber threats.

References

1. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in Proc. IEEE Symp. on Security and Privacy, 2010, pp. 305-316.
2. A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, 2016.
3. P. García-Teodoro et al., "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computers & Security, vol. 28, no. 1, pp. 18-28, 2009.
4. H. Patel, S. Prajapati, and P. Chaudhary, "Intrusion Detection System Using Machine Learning Models," in Proc. Int’l Conf. on Advances in Computing, Communications and Informatics (ICACCI), 2018, pp. 2065-2071.

5. E. F. Nakamura et al., "A Survey on Intrusion Detection Systems," IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 13-35, 2008.
6. Y. Zhang, S. Yu, and S. Nepal, "An Effective Intrusion Detection System Using Multiple Kernel Learning Approach," Future Generation Computer Systems, vol. 79, pp. 473-487, 2018.
7. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1-58, 2009.
8. F. W. D. Wang, K. T. Fung, and L. Zheng, "Using Long Short-Term Memory Recurrent Neural Networks for Network Intrusion Detection," in Proc. IEEE Int'l Conf. on Security, Privacy and Anonymity in Computation, Communication and Storage, 2017, pp. 111-118.
9. M. Z. Alom et al., "Deep Learning for Anomaly Detection: A Survey," IEEE Access, vol. 7, pp. 120134-120148, 2019.
10. W. Sultani, C. Chen, and M. Shah, "Real-World Anomaly Detection in Surveillance Videos," in Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 6479-6488.
11. T. Nguyen, H. Yoo, and K. Kim, "Deep Reinforcement Learning for Cyber Security," IEEE Access, vol. 7, pp. 41913-41930, 2019.
12. C. Shen, X. Li, and H. Lu, "Attack-Resistant Reinforcement Learning for Network Security," Computer Networks, vol. 180, pp. 107363, 2020.
13. B. Biggio, I. Corona, and G. Fumera, "Security Evaluation of Pattern Classifiers Under Attack," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 4, pp. 984-996, 2014.
14. A. P. Dempster et al., "Privacy-Preserving Machine Learning for Cyber Security," in Proc. Int’l Conf. on Information Security, 2019, pp. 189-205.
15. B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proc. Int’l Conf. on Artificial Intelligence and Statistics, 2017, pp. 1273-1282.