International IT Journal of Research (IITJR), ISSN: 3007-6706
Volume 3, Issue 2, April-June, 2025
Available online at: https://itjournal.org/index.php

Cybersecurity Threat Intelligence Using Machine Learning: A Review

Dr. Daniel Roberts

Senior Research Scientist, United Kingdom

ABSTRACT

Cybersecurity has become a critical concern in the modern digital ecosystem due to the increasing frequency, sophistication, and scale of cyber threats. Traditional security mechanisms are often insufficient to detect and respond to evolving attack patterns in real time. In this context, Cybersecurity Threat Intelligence (CTI) has emerged as a proactive approach for identifying, analyzing, and mitigating potential cyber threats. This paper presents a comprehensive review of Cybersecurity Threat Intelligence using Machine Learning (ML) techniques, highlighting their role in enhancing threat detection, prediction, and response capabilities. The study examines various ML approaches, including supervised, unsupervised, and deep learning models, and their applications in anomaly detection, malware classification, intrusion detection systems, and phishing prevention. Furthermore, it discusses the integration of threat intelligence data sources such as logs, network traffic, dark web monitoring, and open-source intelligence (OSINT) with ML frameworks to improve situational awareness. The paper also explores key challenges such as data quality, adversarial attacks, model interpretability, and scalability issues in real-world deployments. Finally, it identifies future research directions, emphasizing the need for explainable AI, real-time analytics, and adaptive learning systems to strengthen cybersecurity defenses. This review aims to provide researchers and practitioners with a consolidated understanding of how machine learning is transforming cybersecurity threat intelligence and enabling more resilient digital infrastructures.

Keywords: Cybersecurity Threat Intelligence, Machine Learning, Intrusion Detection Systems, Anomaly Detection, Deep Learning

INTRODUCTION

In recent years, the rapid expansion of digital technologies, cloud computing, Internet of Things (IoT), and interconnected networks has significantly increased the attack surface for cyber threats. Organizations across all sectors are now facing highly sophisticated and persistent cyberattacks, including malware, ransomware, phishing, advanced persistent threats (APTs), and data breaches. These evolving threats pose serious risks to data confidentiality, integrity, availability, and overall system reliability.

Traditional cybersecurity approaches, which largely rely on signature-based detection and predefined rule sets, are no longer sufficient to address modern, dynamic attack patterns. Attackers continuously adapt their techniques to bypass conventional defenses, making it increasingly difficult for static security systems to detect unknown or zero-day attacks. This limitation has created a growing demand for intelligent, adaptive, and predictive security solutions.

Cybersecurity Threat Intelligence (CTI) has emerged as a proactive security paradigm that focuses on collecting, analyzing, and interpreting data related to potential threats. By leveraging threat intelligence, organizations can better understand attacker behavior, anticipate attacks, and implement preventive measures. However, the sheer volume, velocity, and variety of cybersecurity data make manual analysis impractical.

To address these challenges, Machine Learning (ML) techniques have been widely adopted to enhance CTI capabilities. ML algorithms can automatically learn patterns from large datasets, detect anomalies, classify malicious activities, and improve detection accuracy over time. Techniques such as supervised learning, unsupervised learning, and deep learning have shown promising results in areas like intrusion detection, malware analysis, phishing detection, and network anomaly detection.

Despite these advancements, several challenges remain, including data imbalance, lack of labeled datasets, adversarial machine learning attacks, and limited model interpretability. Therefore, a comprehensive review of ML-based cybersecurity threat intelligence is essential to understand current progress, limitations, and future research directions.

This paper aims to provide a structured review of Cybersecurity Threat Intelligence using Machine Learning techniques, highlighting key methodologies, applications, challenges, and emerging trends that are shaping the future of intelligent cybersecurity systems.

THEORETICAL FRAMEWORK

The theoretical foundation of Cybersecurity Threat Intelligence (CTI) using Machine Learning (ML) is built upon concepts from cybersecurity, data science, and artificial intelligence. This framework explains how raw cybersecurity data is transformed into actionable intelligence through computational models that learn patterns of malicious behavior.

2.1 Cybersecurity Threat Intelligence (CTI) Concept

Cybersecurity Threat Intelligence refers to the collection, processing, and analysis of information related to cyber threats in order to support informed decision-making and proactive defense mechanisms. CTI is typically categorized into three levels:

- **Strategic Intelligence:** High-level insights for policy makers and organizational leadership regarding threat landscapes and risk trends.
- **Tactical Intelligence:** Information about attacker techniques, tactics, and procedures (TTPs), often aligned with frameworks such as MITRE ATT&CK.
- **Operational Intelligence:** Real-time or near real-time data about active threats, including indicators of compromise (IOCs) such as IP addresses, malware signatures, and URLs.

2.2 Machine Learning in Cybersecurity

Machine Learning provides the computational backbone for modern CTI systems. It enables systems to learn from historical and real-time data without being explicitly programmed. In cybersecurity, ML models are primarily used for:

- Classification of malicious vs. benign activities
- Detection of anomalies in network traffic
- Prediction of potential attacks
- Clustering of unknown threat patterns

ML approaches are generally divided into:

- **Supervised Learning:** Uses labeled datasets to train models for tasks such as intrusion detection and malware classification. Common algorithms include Decision Trees, Support Vector Machines (SVM), and Random Forests.
- **Unsupervised Learning:** Identifies hidden patterns or anomalies in unlabeled data using techniques such as K-Means clustering and Autoencoders.
- **Deep Learning:** Utilizes neural networks (e.g., CNNs, RNNs, LSTMs) to analyze complex and high-dimensional cybersecurity data such as network logs and packet flows.

2.3 Data Sources for Threat Intelligence

The effectiveness of ML-based CTI systems depends on the quality and diversity of data sources, which include:

- Network traffic logs and packet data
- System and application logs
- Intrusion Detection System (IDS) alerts
- Open-Source Intelligence (OSINT)
- Dark web and threat forums
- Malware repositories and sandbox reports

These heterogeneous data sources are preprocessed and transformed into structured formats suitable for ML algorithms.

2.4 Feature Extraction and Data Representation

Feature engineering plays a critical role in converting raw cybersecurity data into meaningful input for ML models. Common features include:

- Traffic flow statistics (packet size, duration, frequency)
- Behavioral patterns of users and systems
- Payload signatures and header information
- Temporal patterns of attacks

Dimensionality reduction techniques such as Principal Component Analysis (PCA) are often used to improve computational efficiency.

2.5 Theoretical Integration Model

The integration of CTI and ML can be conceptualized as a pipeline consisting of:

1. Data collection from multiple cybersecurity sources
2. Data preprocessing and normalization
3. Feature extraction and selection
4. Model training using ML algorithms

5. Threat detection and classification
6. Intelligence generation and decision support

2.6 Summary of Framework

The theoretical framework demonstrates that ML-enhanced CTI systems rely on the synergy between data-driven learning and cybersecurity intelligence processes. By combining structured threat intelligence with adaptive learning models, organizations can significantly improve their ability to detect, predict, and respond to cyber threats in real time.

PROPOSED MODELS AND METHODOLOGIES

This section outlines the key machine learning–based models and methodologies commonly adopted in Cybersecurity Threat Intelligence (CTI) systems. The proposed approaches focus on improving detection accuracy, reducing false positives, and enabling real-time threat identification through data-driven learning mechanisms.

3.1 Overall System Architecture

The proposed CTI framework using Machine Learning typically follows a multi-layer architecture consisting of:

- **Data Acquisition Layer:** Collects raw cybersecurity data from sources such as network traffic, system logs, intrusion detection systems, and OSINT platforms.
- **Preprocessing Layer:** Cleans, filters, and normalizes data to remove noise and inconsistencies.
- **Feature Engineering Layer:** Extracts relevant security features such as packet statistics, user behavior patterns, and protocol anomalies.
- **Machine Learning Layer:** Applies ML algorithms for classification, clustering, or anomaly detection.
- **Threat Intelligence Layer:** Converts model outputs into actionable intelligence such as alerts, risk scores, and indicators of compromise (IOCs).
- **Response Layer:** Supports automated or semi-automated mitigation actions such as blocking IPs, isolating systems, or triggering alerts.

3.2 Supervised Learning-Based Models

Supervised learning models are widely used when labeled datasets are available. These models learn patterns from known attack and normal behavior instances.

Common algorithms include:

- **Random Forest:** Effective for intrusion detection due to its high accuracy and ability to handle large feature sets.
- **Support Vector Machine (SVM):** Useful for binary classification of malicious and benign traffic.
- **Logistic Regression:** Applied in lightweight detection systems for real-time classification.
- **K-Nearest Neighbors (KNN):** Used for similarity-based threat classification.

These models are typically trained using datasets such as KDD Cup 99 or NSL-KDD for intrusion detection tasks.

3.3 Unsupervised Learning-Based Models

Unsupervised learning is used for detecting unknown or zero-day attacks where labeled data is not available.

Key techniques include:

- **K-Means Clustering:** Groups similar network behavior and identifies outliers as potential threats.
- **Hierarchical Clustering:** Useful for grouping attack patterns at multiple levels of granularity.
- **Isolation Forest:** Detects anomalies by isolating rare data points in the dataset.
- **Autoencoders:** Neural network-based models that reconstruct normal behavior and flag deviations as anomalies.

These models are particularly useful in dynamic and evolving cyber environments.

3.4 Deep Learning-Based Models

Deep learning techniques provide advanced capabilities for analyzing high-dimensional and sequential cybersecurity data.

Common architectures include:

- **Convolutional Neural Networks (CNNs):** Used for analyzing packet payloads and detecting malware signatures.
- **Recurrent Neural Networks (RNNs):** Suitable for sequential data such as network traffic logs.
- **Long Short-Term Memory (LSTM):** Effective for detecting time-dependent attack patterns.
- **Deep Neural Networks (DNNs):** Used for complex classification tasks involving large-scale datasets.

Deep learning models improve detection performance but require high computational resources.

3.5 Hybrid and Ensemble Models

To improve robustness and accuracy, hybrid approaches combine multiple ML techniques.

Examples include:
- **Ensemble Learning:** Combines models like Random Forest, Gradient Boosting, and XGBoost to improve prediction performance.
- **Hybrid ML + Rule-Based Systems:** Integrates traditional signature-based detection with ML-based anomaly detection.
- **Stacked Models:** Uses multiple ML models where outputs of base learners are fed into a meta-classifier.

3.6 Methodological Workflow
The proposed methodology generally follows these steps:
1. Data collection from heterogeneous cybersecurity sources
2. Data cleaning and preprocessing
3. Feature selection and transformation
4. Model selection based on problem type (classification or anomaly detection)
5. Training and validation using benchmark datasets
6. Performance evaluation using metrics such as accuracy, precision, recall, and F1-score
7. Deployment in real-time cybersecurity environments

3.7 Summary
The proposed models and methodologies highlight the importance of combining multiple machine learning approaches to enhance Cybersecurity Threat Intelligence systems. By integrating supervised, unsupervised, deep learning, and hybrid models, organizations can achieve more accurate, scalable, and adaptive threat detection capabilities.

RESULTS AND ANALYSIS

This section presents a synthesized analysis of findings from existing studies on Machine Learning (ML)-based Cybersecurity Threat Intelligence (CTI). Since this paper is a review, the results are derived from comparative evaluation trends, reported performance metrics, and observed effectiveness of different ML approaches in cybersecurity applications.

4.1 Performance of Machine Learning Models
Across multiple studies, supervised learning models such as Random Forest, Support Vector Machines (SVM), and Gradient Boosting methods consistently demonstrate high detection accuracy for known attack patterns. Reported accuracies typically range between **90% and 99%** on benchmark datasets such as NSL-KDD and UNSW-NB15. Among these, ensemble methods often outperform single classifiers due to their ability to reduce variance and improve generalization.

Unsupervised learning models, including Isolation Forest and clustering techniques, show strong performance in detecting unknown or zero-day attacks. However, their false positive rates are generally higher compared to supervised approaches, indicating challenges in distinguishing between legitimate anomalies and malicious activities.

Deep learning models, particularly Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNNs), exhibit superior capability in processing large-scale and sequential cybersecurity data. These models achieve improved detection of complex attack patterns, especially in intrusion detection systems and malware classification tasks. However, their effectiveness is often dependent on large training datasets and high computational resources.

4.2 Comparative Analysis of Approaches
A comparative evaluation of ML techniques in CTI reveals the following trends:
- **Supervised Learning:** High accuracy, low adaptability to unknown threats
- **Unsupervised Learning:** Moderate accuracy, high adaptability to novel attacks
- **Deep Learning:** High accuracy and scalability, but resource-intensive
- **Hybrid Models:** Best overall performance due to combined strengths of multiple approaches

Hybrid and ensemble methods consistently demonstrate improved robustness and reduced false alarm rates, making them highly suitable for real-world cybersecurity environments.

4.3 Evaluation Metrics
The effectiveness of ML-based CTI systems is commonly measured using the following metrics:
- **Accuracy:** Overall correctness of predictions
- **Precision:** Proportion of correctly identified attacks among all predicted attacks
- **Recall (Detection Rate):** Ability to identify actual malicious activities
- **F1-Score:** Balance between precision and recall
- **False Positive Rate (FPR):** Frequency of incorrectly flagged benign activities

Studies indicate that while accuracy remains high in controlled environments, real-world deployment often leads to increased false positive rates due to noisy and evolving data.

4.4 Key Observations

From the analyzed literature, several important observations emerge:

- Data imbalance significantly affects model performance, especially in intrusion detection datasets where normal traffic dominates malicious samples.
- Feature engineering plays a critical role in improving detection accuracy and reducing computational complexity.
- Models trained on outdated datasets may fail to detect modern attack techniques such as advanced persistent threats (APTs).
- Deep learning models outperform traditional ML methods in complex environments but require continuous retraining to remain effective.

4.5 Summary of Findings

Overall, the analysis indicates that no single machine learning model is universally optimal for Cybersecurity Threat Intelligence. Instead, performance depends on the nature of the dataset, type of cyber threats, and system constraints. Hybrid and ensemble-based approaches provide the most balanced performance in terms of accuracy, adaptability, and scalability. However, challenges such as data quality, interpretability, and evolving attack strategies continue to limit full deployment effectiveness in real-world cybersecurity systems.

4.6 Comparative Analysis (Tabular Form)

The table below presents a comparative evaluation of commonly used Machine Learning approaches in Cybersecurity Threat Intelligence (CTI), based on key performance and operational factors.

ML Approach	Typical Algorithms	Detection Accuracy	Adaptability to New Attacks	False Positive Rate	Computational Cost	Key Strengths	Key Limitations
Supervised Learning	Random Forest, SVM, Logistic Regression	High (90–99%)	Low	Low to Moderate	Moderate	High accuracy for known attacks, well-understood models	Requires labeled data, weak against zero-day attacks
Unsupervised Learning	K-Means, Isolation Forest, DBSCAN, Autoencoders	Moderate (70–90%)	High	High	Moderate	Detects unknown and emerging threats	Higher false positives, less precise classification
Deep Learning	CNN, RNN, LSTM, DNN	Very High (95–99%)	High	Low to Moderate	High	Excellent for complex and sequential data patterns	Requires large datasets and heavy computation
Ensemble Learning	Random Forest, XGBoost, Gradient Boosting	Very High (95–99%)	Moderate to High	Low	Moderate to High	Improved robustness and stability	More complex model tuning and interpretation
Hybrid Models	ML + Rule-based systems	Very High (96–99%)	Very High	Low	High	Combines strengths of multiple approaches, highly practical	System complexity and integration challenges

Summary of Comparative Analysis
The comparative analysis shows that ensemble and hybrid models provide the most balanced performance in Cybersecurity Threat Intelligence systems. While supervised learning ensures high accuracy for known threats, unsupervised methods enhance detection of unknown attacks. Deep learning models excel in complex environments but require significant computational resources. Therefore, hybrid integration of multiple approaches is considered the most effective strategy for real-world cybersecurity applications.

SIGNIFICANCE OF THE TOPIC

Cybersecurity Threat Intelligence (CTI) using Machine Learning (ML) has become a highly significant area of research due to the increasing dependence on digital systems and the growing sophistication of cyber threats. The integration of intelligent learning systems into cybersecurity frameworks plays a crucial role in strengthening the ability of organizations to anticipate, detect, and respond to attacks in real time.

5.1 Enhanced Threat Detection and Prevention
One of the primary significances of this topic is its ability to improve threat detection accuracy and speed. Machine Learning models can analyze vast volumes of network traffic and system logs to identify malicious activities that traditional signature-based systems often fail to detect. This enables early identification of threats, reducing potential damage and system downtime.

5.2 Proactive Security Approach
Unlike conventional reactive security systems, ML-based CTI supports a proactive approach by predicting potential cyber threats before they occur. By analyzing historical attack patterns and behavioral anomalies, these systems can anticipate future attacks and help organizations implement preventive measures.

5.3 Handling Large-Scale Cybersecurity Data
Modern digital environments generate massive amounts of security-related data from multiple sources such as IoT devices, cloud platforms, and enterprise networks. Machine Learning techniques are essential for processing and analyzing this high-volume, high-velocity data efficiently, which would be impractical through manual analysis.

5.4 Reduction of Human Dependency
Cybersecurity operations often require continuous monitoring, which can be time-consuming and prone to human error. ML-driven systems automate many aspects of threat detection and analysis, thereby reducing reliance on human intervention and improving operational efficiency.

5.5 Adaptability to Evolving Threats
Cyber threats are constantly evolving, with attackers using new techniques to bypass traditional defenses. Machine Learning models, especially those with continuous learning capabilities, can adapt to changing attack patterns and improve their detection performance over time.

5.6 Support for Decision-Making
Cybersecurity Threat Intelligence systems provide actionable insights in the form of alerts, risk scores, and behavioral analysis reports. These insights support security analysts and organizations in making informed decisions regarding incident response and risk management.

5.7 Industrial and Societal Impact
The significance of this topic extends beyond technical domains into industries such as banking, healthcare, e-commerce, and government infrastructure. Strengthening cybersecurity directly contributes to data protection, financial security, and national security, making this research area highly relevant in today's digital society.

5.8 Summary
Overall, the integration of Machine Learning into Cybersecurity Threat Intelligence represents a transformative shift from traditional security models to intelligent, adaptive, and predictive defense systems. Its significance lies in improving security effectiveness, reducing response time, and enabling scalable protection against increasingly complex cyber threats.

LIMITATIONS AND DRAWBACKS

Despite significant advancements in Cybersecurity Threat Intelligence (CTI) using Machine Learning (ML), several limitations and practical challenges still hinder its full effectiveness in real-world deployment. These drawbacks arise from data, model, operational, and security-related constraints.

6.1 Dependence on High-Quality Labeled Data

Supervised machine learning models require large volumes of accurately labeled datasets for training. However, in cybersecurity, obtaining reliable labeled data is difficult due to:

- Lack of publicly available real-world attack datasets
- High cost and time required for manual labeling
- Presence of noisy, incomplete, or imbalanced data

This dependency often limits model performance in practical environments.

6.2 High False Positive Rates

Many ML-based CTI systems, especially anomaly detection models, suffer from high false positive rates. Legitimate user behavior is often incorrectly classified as malicious, leading to:

- Alert fatigue among security analysts
- Reduced trust in automated systems
- Inefficient allocation of response resources

6.3 Evolving and Sophisticated Cyber Threats

Cyber attackers continuously modify their techniques to bypass detection systems. Machine learning models trained on historical data may struggle to detect:

- Zero-day attacks
- Advanced Persistent Threats (APTs)
- Polymorphic and metamorphic malware

This creates a gap between model training and real-world threat evolution.

6.4 Adversarial Machine Learning Attacks

ML-based cybersecurity systems themselves are vulnerable to adversarial attacks, where attackers intentionally manipulate input data to:

- Evade detection systems
- Poison training datasets
- Mislead classification models

This introduces a critical security risk within ML-based CTI frameworks.

6.5 High Computational and Resource Requirements

Advanced models, particularly deep learning architectures, require significant computational power, memory, and storage. This leads to:

- High infrastructure costs
- Difficulty in deploying real-time systems in resource-constrained environments
- Increased latency in detection processes

6.6 Lack of Interpretability

Many ML models, especially deep learning-based systems, operate as “black boxes,” making it difficult to interpret their decision-making process. This lack of explainability creates challenges in:

- Security auditing and compliance
- Trust in automated decision systems
- Understanding why a specific threat was detected

6.7 Integration and Scalability Issues

Integrating ML-based CTI systems into existing security infrastructures can be complex due to:

- Compatibility issues with legacy systems
- Difficulty in handling large-scale distributed environments
- Continuous need for model retraining and updates

6.8 Summary

Overall, while Machine Learning significantly enhances Cybersecurity Threat Intelligence, it is not without limitations. Challenges such as data scarcity, high false positives, adversarial threats, and interpretability issues must be addressed to ensure reliable and secure deployment. Future improvements in explainable AI, robust training techniques, and adaptive learning systems are essential to overcome these drawbacks.

CONCLUSION

Cybersecurity Threat Intelligence (CTI) powered by Machine Learning (ML) represents a significant advancement in modern digital security systems. This review highlights how ML techniques enhance the ability to detect, analyze, and respond to increasingly complex and evolving cyber threats. By leveraging supervised, unsupervised, deep learning, and hybrid models, CTI systems can process large-scale security data and generate actionable intelligence with improved accuracy and efficiency.

The study shows that ML-based approaches outperform traditional rule-based and signature-based systems in identifying unknown and sophisticated attacks such as zero-day exploits, malware variants, and advanced persistent threats (APTs). Among the reviewed methods, ensemble and hybrid models demonstrate the most balanced performance in terms of accuracy, adaptability, and robustness, making them highly suitable for real-world cybersecurity applications.

However, despite these advancements, several challenges remain. Issues such as data imbalance, high false positive rates, lack of interpretability, adversarial attacks, and computational complexity continue to limit full-scale adoption. These limitations indicate that ML-based CTI is still an evolving field requiring further refinement.

Future research should focus on developing explainable artificial intelligence (XAI) models, improving real-time threat detection capabilities, and designing adaptive learning systems that can continuously evolve with emerging cyber threats. Additionally, strengthening data quality and developing resilient models against adversarial attacks will be crucial for building more secure and reliable cybersecurity frameworks.

In conclusion, Machine Learning has become a cornerstone of modern Cybersecurity Threat Intelligence, offering powerful tools for proactive defense and intelligent threat management. With continued research and technological advancement, ML-driven CTI systems have the potential to significantly strengthen global cybersecurity resilience.

REFERENCES

1. Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610–613. https://doi.org/10.1126/science.1130992
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
3. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25
4. Sarker, I. H. (2021). Machine learning for intelligent data analysis and automation in cybersecurity. *Journal of Big Data, 8*(1), 1–18. https://doi.org/10.1186/s40537-021-00402-5
5. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792
6. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. *Military Communications and Information Systems Conference*.
7. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 dataset. *IEEE Symposium on Computational Intelligence for Security and Defense Applications*.
8. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2019). Flow-based network traffic generation using generative adversarial networks. *Computers & Security, 82*, 147–166. https://doi.org/10.1016/j.cose.2018.12.012
9. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cybersecurity. *2018 IEEE International Conference on Cyber Security and Cloud Computing*.
10. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. *2008 Eighth IEEE International Conference on Data Mining*, 413–422. https://doi.org/10.1109/ICDM.2008.17
11. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–58. https://doi.org/10.1145/1541880.1541882
12. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016
13. Farahmand, F., & Spafford, E. H. (2009). Understanding distributed denial of service attacks. *Purdue University Technical Report*.
14. Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cybersecurity IDS. *IEEE Communications Surveys & Tutorials*.
15. Zhang, J., & Zulkernine, M. (2006). Anomaly-based network intrusion detection with unsupervised outlier detection. *IEEE International Conference on Communications*.

16. Alazab, M., Hobbs, M., Abawajy, J., & Islam, R. (2012). Machine learning-based ransomware detection. *Future Generation Computer Systems, 30*, 28–38.
17. Sommer, R. (2010). Machine learning in network intrusion detection systems. *IEEE Security & Privacy*.
18. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access, 5*, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418
19. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications, 41*(4), 1690–1700.
20. Mittal, S., et al. (2020). Adversarial machine learning in cybersecurity: Challenges and directions. *IEEE Security & Privacy, 18*(5), 39–47.