# Harnessing Machine Learning for APTs Detection and Mitigation in Large-Scale Networks

Reeta Mishra
*Department of Computer Science & Technology*
*Manav Rachna University*
Faridabad, Haryana, India
https://orcid.org/0009-0001-7219-425X

Neelu Chauduray
*Department of Computer Science & Technology,*
*Manav Rachna University*
Faridabad, Haryana, India
neelu@mru.edu.in

Gaganjot Kaur
*Department of Computer Science*
*Raj Kumar Goel Institute of Technology*
Ghaziabad (U.P.), India
gaganjot28784@gmail.com

2024 7th International Conference on Contemporary Computing and Informatics (IC3I) | 979-8-3503-5006-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/IC3I61595.2024.10829149

***Abstract*— A significant and ongoing cyber security concern is the presence of Advanced Persistent Threats (APTs), especially in large-scale networks. APTs are known for their lengthy lifespan, stealth, and sophistication. As a result, they frequently elude conventional security measures, calling for more flexible and durable solutions. Machine learning (ML) has become a potent instrument for improving these sophisticated threats' detection and response. This review paper investigates the use of machine learning (ML) to counteract advanced persistent threats (APTs), emphasizing critical techniques including anomaly detection, behavioural analysis, and threat intelligence integration. We investigate how successfully different machine learning algorithms—such as deep learning models, supervised, unsupervised, and reinforcement learning approaches—identify and react to APT activities. The paper also discusses important obstacles to overcome when using machine learning (ML) for APT detection, such as problems with data quantity and quality, attacker evasion strategies, scalability issues, and more. We highlight the advantages and disadvantages of existing ML-based techniques in practice using real-world examples. The report also addresses future areas for research, highlighting the necessity of improved model robustness, adaptive learning capabilities, and cooperative efforts to remain ahead of developing cyber threats. With an emphasis on both the state of the art and potential directions for future research, this review seeks to give readers a thorough grasp of how machine learning (ML) can be used to fortify cyber security defences against advanced persistent threats (APTs) in large-scale network systems.**

***Keywords*— *Machine learning, advanced persistent threat, detection, threat intelligence, large-scale networks, multi-stage attack***

## I. INTRODUCTION

The modern digital age has seen previously unheard-of improvements in communication, business, and information exchange due to our growing reliance on networked technologies and the internet. But with this digital revolution came more sophisticated cyber dangers; one of the most pernicious and difficult to counter is Advanced Persistent dangers (APTs). The targeted character of APTs is evident in their frequent focus on high-value targets like governmental bodies, financial institutions, and suppliers of vital infrastructure. APTs take a longer, more methodical approach than ordinary cyber attacks, which are usually swift and opportunistic. Attackers meticulously plot their actions, carrying out in-depth reconnaissance to find weaknesses, creating several bases of operations, and using a variety of strategies to evade discovery. Once they enter the network, they cause disruption or steal confidential information while staying hidden. Antivirus software, intrusion detection systems (IDS), and firewalls are examples of traditional cyber security methods that have not shown to be effective against advanced persistent threats. Due to their primary reliance on established criteria and recognised signatures, these technologies are unable to effectively counteract the innovative and adaptable techniques employed by APT actors. Because APTs are dynamic and constantly changing, we need more sophisticated and flexible security systems that can quickly detect and neutralise these threats. Potential for ML-driven adaptive cyber defence as a proactive and dynamic strategy to counter APTs [14]. Enhancing APT detection and mitigation with machine learning (ML) has shown promise.

Machine learning (ML) is able to identify trends and anomalies that could point to malicious activities by utilising large datasets and advanced algorithms. ML-based systems, in contrast to conventional techniques, offer proactive protection against APTs by being able to learn from previous instances and adjust to changing threat environments. The approach suggested by [5] attempts to detect unusual patterns and behaviours suggestive of cyber threats before they materialise into actual attacks. In the area of cyber security, machine learning algorithms provide several benefits. Accurate threat identification is made possible by supervised learning algorithms that may be trained on labelled datasets to distinguish between benign and malicious activity. In the multi-layered defence strategy included in the [4] suggested framework, deep learning models are used at several stages of the cyber security protocol, from early threat detection to final incident response. Deep learning models are a major breakthrough in cyber security that provide improved threat detection and mitigation capabilities.

Conversely, unsupervised learning techniques are superior at spotting abnormalities because they can distinguish patterns that depart from typical behavior without needing to be aware of particular dangers beforehand. By allowing models to learn from their interactions with the environment and unearth intricate data structures, deep learning and reinforcement learning further expand on machine learning's capabilities. Despite ML's promise to tackle APTs, a number of issues must be resolved before its full benefits may be realized. An Inference-Based Adaptive Attack Tolerance (IBAAT) system with two stages is developed by [3]. A forward-backward algorithm with a temporal window is used to conduct a security risk assessment in the first step. In the second stage, the assault and defensive process is modelled as a two-player general-sum Markov game, and the best defence plan is determined by quantitative analysis using the data from the previous stage. Based on the evaluation, the suggested algorithm



979-8-3503-5006-7/24/$31.00 ©2024 IEEE

Authorized licensed use limited to: RNS Institute of Technology. Downloaded on March 07,2025 at 13:51:07 UTC from IEEE Xplore. Restrictions apply.

outperforms the state-of-the-art by roughly 10% regarding security utility.

Comparing the suggested algorithm to the state-of-the-art, the evaluation reveals a security utility improvement of roughly 10% . According to the evaluation, the suggested algorithm outperforms the state-of-the-art by roughly 10% regarding security usefulness. Based on the evaluation, the suggested algorithm outperforms the state-of-the-art by roughly 10% in terms of security utility. The quantity and quality of data needed to train efficient machine learning models is a significant obstacle. Since APTs are somewhat uncommon, it can be challenging to find tagged data that is unique to these threats. Furthermore, noise and imbalances are common in network data, which might affect how well ML algorithms work. Significant obstacles are also presented by the evasion strategies used by attackers, such as adversarial attacks and zero-day exploits. Another crucial concern is scalability, since massive networks produce enormous volumes of data that must be processed instantly. For fast threat detection and response, low latency and effective processing are critical requirements. In order to prevent overburdening security staff with alerts and guarantee that harmful activity is not overlooked, it is also essential to strike a balance between false positives and false negatives. In order to detect and mitigate APTs in large-scale networks, this review paper attempts to give a thorough overview of the application of ML. To highlight the usefulness and drawbacks of these approaches, we will examine a variety of machine learning techniques, evaluate their efficacy, and provide practical examples. The study will also review future paths for research, highlighting the need for improved model resilience, adaptive learning capabilities, and teamwork to keep up with changing cyber threats. This work aims to illustrate the promise as well as the constraints of these methods by analysing the state of ML applications in APT detection and mitigation. In addition, we will highlight the necessity for cooperation between government, business, and academia in order to keep abreast of the ever-evolving cyber threat landscape and suggest future research directions.

### *A. Advanced Persistent Threats*

The intricacy and persistence of APTs are distinct. APTs, in contrast to typical cyber attacks, take several stages, such as data exfiltration, lateral movement, exploitation, and initial reconnaissance. To avoid detection and accomplish the attacker's goals, each stage is meticulously carried out.

1. Stealthiness. They employ complex strategies to avoid being discovered by traditional security technologies.
2. Targeted Nature: APTs are typically aimed at particular industries or companies, frequently with valuable assets.
3. Extended Duration: APTs may go unnoticed for several months or even a few years. 4. Resource-intensive: These attacks are usually supported by well-organised, well-funded groups, occasionally with state sponsorship. It is essential to comprehend these traits in order to create detection and mitigation plans that work. Recursive Feature Elimination (RFE) was the main technique utilised by [2] in feature selection to improve intrusion detection system performance.

### *B. Life Cycle of Advanced Persistent Threats (APTs)*

The stages of the APT life cycle include initial reconnaissance, access acquisition, foothold establishment, privilege escalation, data exfiltration, and persistence maintenance; stealth tactics are frequently employed to evade detection while carrying out the assault. Refer to Table 1 for more details:

TABLE I. OVERVIEW OF THE APT LIFE CYCLE, HIGHLIGHTING OBJECTIVES, TECHNIQUES, AND OUTCOMES

| Phase | Objective | Techniques | Outcome |
|---|---|---|---|
| Initial Reconnaissance | Gather intelligence about target | Social engineering, OSINT, network scanning | Detailed knowledge of target environment, including IP addresses, domain names, and entry points |
| Initial Compromise | Gain a foothold in the network | Phishing emails, exploiting public-facing vulnerabilities, drive-by downloads, zero-day exploits | Establishment of an initial access point, often through compromised credentials or malware |
| Establishing Persistence | Maintain long-term access | Installing backdoors, root kits, or persistent malware | Persistent presence within the network, allowing continued access |
| Privilege Escalation | Gain higher-level access | Exploiting system vulnerabilities, leveraging stolen credentials, lateral movement | Elevated privileges enabling more extensive network control |
| Internal Reconnaissance | Understand internal structure | Network mapping, scanning for vulnerabilities, monitoring internal communications | Comprehensive knowledge of network layout and valuable assets |
| Lateral Movement | Move within the network | Using stolen credentials, exploiting trust relationships, and remote administration tools | Spread of attack across network, accessing multiple systems and data repositories |
| Data Exfiltration | Extract valuable data | Compressing, encrypting, and covertly transferring data to external servers | Successful extraction of sensitive information or other valuable assets |
| Maintaining Presence | Ensure ongoing access | Setting up redundant access points, planting additional backdoors, and using legitimate tools | Continued access for future operations |



Authorized licensed use limited to: RNS Institute of Technology. Downloaded on March 07,2025 at 13:51:07 UTC from IEEE Xplore. Restrictions apply.

| Phase | Objective | Techniques | Outcome |
|---|---|---|---|
| Covering Tracks | Evade detection | Deleting logs, altering timestamps, using anti-forensic tools, and hiding malware and traffic | Minimization of forensic evidence, hindering detection and understanding of intrusion |

### C. Machine Learning in Cyber Security

Cybersecurity has been transformed by machine learning, among other sectors. Utilising machine learning techniques, we are able to examine enormous volumes of data, spot trends, and forecast any dangers. According to [28], machine learning models are vulnerable to a variety of attacks, which puts the models and the systems they protect in serious danger. A novel architecture called SecurityBERT is presented by [13] to detect cyber threats in the Internet of Things networks by utilising the Bidirectional Encoder Representations from Transformers (BERT).

It surpassed earlier marks set by hybrid solutions like GAN-Transformer-based architectures and CNN-LSTM models with an astounding 98.2% overall accuracy in identifying fourteen distinct assault types. Its small model size of 16.7 MB and inference time of less than 0.15 seconds on a typical CPU make it a good option for deployment on resource-constrained IoT devices as well as for real-world traffic analysis. The methods proposed by [27] are applicable to a wide range of digital domains. These include but are not limited to tasks like malware detection, spam recognition, fraud identification, anomaly detection, phishing attempt detection, Distributed Denial of Service (DDoS) attack detection, and vulnerability discovery. Research trends in this subject, adversarial assaults and defences, and the deep learning-based network intrusion detection system are all explained by [2]).Principal

ML Methods in Cyber security:

1. Supervised learning: Using labelled datasets, models are trained to distinguish between benign and harmful activity.
2. Unsupervised Learning: This method, which does not require prior labelling, finds patterns that differ from typical behaviour in order to detect anomalies.
3. Reinforcement Learning: Over time, models refine their detection and mitigation techniques by learning the best responses via trial and error.
4. Deep Learning: Applying multi-layered neural networks to intricate data structures, this technique offers very accurate threat detection. These methods serve as the cornerstone of contemporary cyber security defences against APTs. Researchers [8] suggested a framework based on multi-layered defence strategies included in the deep learning models that are used at several stages of the cyber security protocol, from early threat detection to final incident response. Deep learning models are a major breakthrough in cyber security that provide improved threat detection and mitigation capabilities. One more researcher scholars incorporating emotional intelligence into human-robot collaboration improves communication, trust, and adaptability. By recognizing and responding to human emotions, robots can create more intuitive interactions, leading to smoother teamwork and enhanced productivity. Researchers [29] introduced block chain-based security solutions to improve cyber security by offering decentralised, unchangeable data verification and storage. They improve data integrity, decrease single points of failure, and increase transparency in safe transactions and communications.

### A. Methodologies for APT Detection Using Machine Learning

By examining network behaviour, spotting abnormalities, and categorising possible threats, machine learning-based APT detection methodologies—which include supervised learning, anomaly detection, clustering, and deep learning techniques—allow for the discovery of complex attack patterns. Refer to Table 2 for details:

TABLE II. EXISTING APT DETECTION METHODS USING M L TECHNIQUES

| Methodology | Objective | Techniques | Application | Strengths | Challenges |
|---|---|---|---|---|---|
| Supervised Learning | Classify activities as benign or malicious. | Decision Trees, SVM, Random Forests, Neural Networks | Use historical data with known attack labels to train models. | High accuracy with well-labelled data, effective for known attack patterns | Requires large labelled datasets, less effective against new threats |
| Unsupervised Learning | Detect anomalies without labelled data | K-Means, DBSCAN, Hierarchical Clustering, Isolation Forest, One-Class SVM | Analyse normal behaviour and identify deviationi indicating threats. | Effective for unknown threats, does not require labelled data | High false positives, distinguishing benign anomalies from threats |
| Semi-supervised learning | Use small labelled and large unlabelled data | Self-training, co-training, semi-supervised SVM | Improve model performance with limited labelled data | Balances need for labelled data, improves accuracy | Performance highly dependent on labelled data quality |
| Reinforcement Learning | Learn optimal strategies through interaction | Q-Learning, Deep Q-Networks (DQN), Policy Gradient methods | Models learn to identify and respond to APT activities from feedback. | Adapts to dynamic environments, learns complex action sequences | Requires well-defined reward structure, time-consuming, computationally intensive |



Authorized licensed use limited to: RNS Institute of Technology. Downloaded on March 07,2025 at 13:51:07 UTC from IEEE Xplore. Restrictions apply.

| Methodology | Objective | Techniques | Application | Strengths | Challenges |
|---|---|---|---|---|---|
| Deep Learning | Automatically learn feature representations | CNN, RNN, LSTM, Autoencoders | Analyse large-scale network traffic, logs, and data sources | Processes large datasets, extracts features from raw data | Requires substantial computational resources, interpretability issues |
| Hybrid Approaches | Combine multiple ML techniques | Integrating supervised, unsupervised, and reinforcement learning; stacking, bagging, boosting | Create robust detection systems by combining methodologies | Enhanced detection performance, balances strengths of various methods | Increased model complexity, higher computational requirements |
| Feature Engineering | Identify relevant features | SVM, KNN, Logistic regression | Fetch malicious behaviour in network traffic, system logs | Classification is easy | Less effective in unstructured data |
| Ensemble Methods | To improve threat detection accuracy and robustness. | Adaboost , XGboost ,Cat boost | Credit score calculation by financial institutions offering a better future plans. | Improve accuracy and robustness. | Requires large labelled datasets |
| Real – time processing | To handle incoming data streams in real-time. | Apache Kafka, Apache Spark. | Splunk used for real-time fraud detection and analytics. | Process incoming data streams in real-time. | Growing data quantities impact the performance of the application. There are serious consequences related to any breaches of data security and privacy. |
| Behavioural Analysis | Focus on deviations from established behavioural norms | HMMs, KNN | Employees monitoring activities within the workplace to prevent data breaches, and unauthorized access. | To identify discrepancies and offer a proactive method of threat detection. | Large volumes of data are required to create precise behavior norms, and privacy concerns |
| Threat Intelligence | Integrate threat intelligence feeds and improve detection accuracy. | Random Forests | FireEye Threat Intelligence | Improve detection accuracy; models trained with up-to-date information on known threats and vulnerabilities. | Huge data is collected, security teams in large networks may become overwhelmed and require the expertise to efficiently assess and prioritize threats. |
| Continuous Learning | Implement mechanisms for model training and updating to adapt evolving APT tactics. | Decision trees, neural networks and Bayesian networks | Adaptive Learning Systems (Education, higher studies) | To prioritize ongoing model learning and improvement. | Data imbalance issue |
| Scalability & performance | Handles large data volumes efficiently and provides real-time results. | Collaborative Filtering | E-commerce recommendation systems | Able to work on large data volumes quietly and efficiently, | Algorithm complexity and privacy concerns |
| Validation & Testing | Regularly validate model effectiveness against all-time data | Simultaneous Localization and Mapping (SLAM), Support Vector Machines | Autonomous Driving, Natural Language Processing (NLP) Sentiment Analysis | Provide effective outcomes against pre-processed new and historical data to ensure reliability and accuracy. | Not effective on limited or very precise data. |

Automated response mechanisms, intrusion detection systems (IDS), anomaly detection, and other EA applications in cyber security were covered by [8]. It explains how to



Authorized licensed use limited to: RNS Institute of Technology. Downloaded on March 07,2025 at 13:51:07 UTC from IEEE Xplore. Restrictions apply.

combine EAs with machine learning models to improve threat intelligence and predictive analytics, which will help anticipate and neutralize more complex threats. The AI models suggested by [11] provide a number of benefits over traditional techniques, including increased accuracy, scalability, and flexibility to changing network conditions. Additionally, by identifying vulnerabilities early on, businesses can take proactive steps to put security measures in place to reduce risks and stop any cyber attacks, strengthening network resilience overall and protecting sensitive data. According to [14], resilient systems are made to endure setbacks and carry on even while enemies are active. According to [6], it explores the state-of-the-art deep learning-based intrusion detection techniques for security.

### B. *Comparative on various Advanced Persistence Threats detection models:*

A comparative analysis of various Advanced Persistent Threat (APT) detection models, focusing on methodologies, effectiveness, accuracy, and challenges in large-scale networks. Refer to Table 3 for more details:

TABLE III. COMPARATIVE ON VARIOUS APTS DETECTION MODELS.

| S.No. | Model | Reference | Dataset | Accuracy /Outcomes |
|---|---|---|---|---|
| 1 | CNN- BiLSTM | [17] | NSL -KDD | 83.58 |
| 2 | SVM-Naïve Bayes | [18] | NSL -KDD | 99.35 |
| 3 | AE-SVM-GO | [20] | NSL -KDD | 99.6 |
| 4 | AE-Triplet Network | [19] | UNSW | NB1592.4 |
| 5 | CRNN | [21] | CSE-CIC-DS2018 | 97.6 |
| 6 | LSTM | [16] | Generated | 99.08 |
| 7 | APT Guard | [15] | Semi-synthetic dataset | 99.89 |
| 8 | Attack pyramid(HMM) | [22] | Semi-synthetic dataset | 91.80 |
| 9 | DT,SVM,K-NN, Ensemble | [23] | | 84.8 |
| 10 | Security system | [24] | Map reduce | Calculate FP rate Co=0.75.0.50,0.25. |
| 11 | TerminAPT | [26] | IDS Data & Alerts | Detected 7.4 attacks /day, during 67 days |

### C. *Applying machine learning to APT detection*

The application of machine learning (ML) in detecting Advanced Persistent Threats (APTs) in large-scale networks is promising but fraught with numerous challenges. These challenges stem from the complexity of APTs, the dynamic nature of cyber threats, and the inherent limitations of ML algorithms. Below, we delve into the primary challenges faced in this domain.

#### 1) *Data Quality and Quantity*

**Data Scarcity**: APT detection requires vast amounts of high-quality data to train ML models effectively. However, obtaining labeled data specific to APTs is difficult due to their rarity and the reluctance of organizations to share incident data.

**Noise and Imbalance**: Network data often contains noise and is imbalanced, with benign activities vastly outnumbering malicious ones. This imbalance can lead to biased models that are less effective at detecting rare APT activities.

**Data Privacy and Security**: Collecting and using network data for ML purposes raises concerns about data privacy and security. Organizations must ensure that sensitive information is protected, which can complicate data collection and processing.

#### 2) *Evasion Techniques*

**Adversarial Attacks**: Attackers continually develop new methods to evade detection, such as adversarial attacks that subtly modify inputs to deceive ML models. Researchers [9] stated smart techniques can significantly reduce the effectiveness of static models.

**Zero-Day Exploits**: APTs often leverage zero-day vulnerabilities, which are unknown to security vendors and researchers. ML models trained on historical data may fail to detect such novel threats.

**Polymorphic and Metamorphic Malware**: Malware used in APTs can change its code structure (polymorphism) or behaviour (metamorphism) to evade signature-based detection and complicate behaviour analysis.

#### 3) *False positives and False Negatives*

**False Positives**: High rates of false positives, where benign activities are incorrectly flagged as malicious, can overwhelm security teams and lead to alert fatigue. This reduces the effectiveness of security operations and can result in genuine threats being overlooked.

**False Negatives**: Conversely, false negatives, where malicious activities go undetected, pose a significant risk as APTs can continue to operate undetected. Balancing the trade-off between false positives and false negatives is a critical challenge.

**Threshold Setting**: Determining appropriate thresholds for anomaly detection and classification models is complex. Too sensitive thresholds can increase false positives, while too lenient thresholds can lead to missed detections.

#### 4) *Model Interpretability and Explainability*

**Black-Box Nature**: Many ML models, especially deep learning algorithms, are considered black boxes, making it difficult to understand and explain their decisions. Lack of interpretability can hinder trust and acceptance by security professionals.

**Regulatory Compliance**: In some industries, regulatory requirements mandate that security decisions be explainable. Ensuring that ML models comply with such regulations while maintaining high detection performance is a challenge.

**Human Expertise**: Security analysts need to understand and verify the alerts generated by ML models. Providing interpretable and actionable insights is essential for effective human-machine collaboration.

#### 5) *Dynamic and Evolving Threat Landscape*

**Rapid Evolution**: The cyber threat landscape evolves rapidly, with new attack techniques and tools emerging continuously. ML models must be regularly updated and retrained to keep pace with these changes, which can be resource-intensive.

**Attack Attribution**: Identifying the source and intent of an APT is complex due to sophisticated obfuscation techniques.



Authorized licensed use limited to: RNS Institute of Technology. Downloaded on March 07,2025 at 13:51:07 UTC from IEEE Xplore. Restrictions apply.

ML models must incorporate advanced threat intelligence and context-aware analysis to improve attribution accuracy.

*6) Integration and Deployment*

**System Integration**: Integrating ML models with existing security infrastructure, such as security information and event management (SIEM) systems and endpoint detection and response (EDR) solutions, can be challenging.

**Deployment Challenges**: Deploying ML models in operational environments requires addressing issues related to model lifecycle management, versioning, and rollback mechanisms to ensure continuity and reliability.

**Real-World Constraints**: ML models must operate within the constraints of real-world environments, including varying network architectures, hardware limitations, and organizational policies. Addressing these challenges requires a multi-faceted approach that combines advancements in ML research with practical considerations in cyber security. Collaboration between academia, industry, and government agencies is essential to developing robust, scalable, and effective solutions for APT detection and mitigation.

*7) Real-Time Examples of ML in APT Detection*

**Detecting Spear Phishing Attacks** A financial institution implemented an ML-based system using Natural Language Processing (NLP) and supervised learning to detect spearphishing emails. The system successfully identified and mitigated several targeted phishing attempts, protecting sensitive financial data.

**Network Traffic Analysis** A multinational corporation deployed an unsupervised learning algorithm to analyse network traffic and detect anomalies. The system identified unusual data transfers indicative of APT activities, leading to the discovery of compromised systems and mitigation of the threat.

**Endpoint Security** An endpoint security solution integrated ML-based behavioural analysis to monitor user activities. The system detected suspicious behaviour patterns, such as unusual login times and access to sensitive files, enabling the organisation to respond swiftly to potential APTs.

*8) Future Directions and Conclusion*

The application of machine learning in APT detection and mitigation is a rapidly evolving field. Future research should focus on enhancing model robustness, improving data quality, and developing adaptive algorithms capable of countering advanced evasion techniques. Collaboration between academia, industry, and government agencies will be essential to stay ahead of sophisticated attackers. In conclusion, machine learning offers promising solutions for detecting and mitigating APTs in large-scale networks. While challenges remain, ongoing advancements in ML and cyber security hold the potential to significantly enhance our ability and awareness to defend against these persistent threats.

## ACKNOWLEDGMENT

We extend our sincere gratitude to Dr. Neelu Chaudhary and Dr. Gaganjot Kaur for their invaluable contributions to the successful completion of this research. We are particularly grateful to Manav Rachna University, Faridabad, Haryana, India, for providing the essential resources and unwavering support. Our heartfelt appreciation also goes to our colleagues and mentors for their insightful feedback and encouragement throughout the research process. Additionally, we wish to thank the anonymous reviewers for their constructive suggestions, which significantly enhanced the quality of this paper. Finally, we acknowledge the critical role of the open-source community and the pioneering researchers whose work provided the foundation for our study on machine learning and APT detection in large-scale networks.

## REFERENCES

[1] Maddireddy, B. R., & Maddireddy, B. R. (2023). Adaptive Cyber Defense: Using Machine Learning to Counter Advanced Persistent Threats. International Journal of Advanced Engineering Technologies and Innovations, 1(03), 305-324.

[2] Kannankeril George, C. L. (2024). Detecting and Mitigating Advanced Persistent Threats using Machine Learning Techniques (Doctoral dissertation, Dublin Business School).

[3] Xie, Y. X., Ji, L. X., Li, L. S., Guo, Z., & Baker, T. (2021). An adaptive defense mechanism to prevent advanced persistent threats. Connection Science, 33(2), 359-379.

[4] Maddireddy, B. R., & Maddireddy, B. R. (2024). Advancing Threat Detection: Utilizing Deep Learning Models for Enhanced Cyber security Protocols. Revista Espanola de Documentacion Cientifica, 18(02), 325-355.

[5] Bai, M., & Fang, X. (2024). Machine learning-based threat intelligence for proactive network security. Integrated Journal of Science and Technology, 1(2).

[6] Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2023). Deep learning for cyber threat detection in IoT networks: A review. Internet of Things and Cyber-Physical Systems.

[7] Olowononi, F. O., Rawat, D. B., & Liu, C. (2020). Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS. IEEE Communications Surveys & Tutorials, 23(1), 524-552.

[8] Maddireddy, B. R., & Maddireddy, B. R. (2020). AI and Big Data: Synergizing to Create Robust Cyber security Ecosystems for Future Networks. International Journal of Advanced Engineering Technologies and Innovations, 1(2), 40-63.

[9] He, K., Kim, D. D., & Asghar, M. R. (2023). Adversarial machine learning for network intrusion detection systems: A comprehensive survey. IEEE Communications Surveys & Tutorials, 25(1), 538-566.

[10] Atadoga, A., Sodiya, E. O., Umoga, U. J., & Amoo, O. O. (2024). A comprehensive review of machine learning's role in enhancing network security and threat detection. World Journal of Advanced Research and Reviews, 21(2), 877-886.

[11] Pala, S. K. Study to Develop AI Models for Early Detection of Network Vulnerabilities. International Journal of Enhanced Research in Science, Technology & Engineering ISSN, 2319-7463.

[12] Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access.

[13] Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., & Lestable, T. (2023). Revolutionizing cyber threat detection with large language models. arXiv preprint arXiv:2306.14263.

[14] Sakthivelu, U., & Vinoth Kumar, C. N. S. (2023). Advanced Persistent Threat Detection and Mitigation Using Machine Learning Model. Intelligent Automation & Soft Computing, 36(3).

[15] Nadim, I., Rajalakshmi, N. R., & Hammadeh, K. (2024). A Novel Machine Learning Model for Early Detection of Advanced Persistent Threats Utilising Semi-Synthetic Network Traffic Data. Journal of VLSI Circuits and Systems, 6(2), 31-39.

[16] Krishnapriya, S., & Singh, S. (2024). A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques.

[17] Hammadeh, K., & Kavitha, M. (2023). Unravelling Ransomware: Detecting Threats with Advanced Machine Learning Algorithms. International Journal of Advanced Computer Science and Applications, 14(9).

[18] Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network intrusion detection combined hybrid sampling with deep hierarchical network. IEEE access, 8, 32464-32476.



Authorized licensed use limited to: RNS Institute of Technology. Downloaded on March 07,2025 at 13:51:07 UTC from IEEE Xplore. Restrictions apply.

[19] Gu, J., & Lu, S. (2021). An effective intrusion detection approach using SVM with naïve Bayes feature embedding. Computers & Security, 103, 102158.

[20] Andresini, G., Appice, A., & Malerba, D. (2021). Autoencoder-based deep metric learning for network intrusion detection. Information Sciences, 569, 706-727.

[21] Chikkalwar, S. R., & Garapati, Y. (2022). Autoencoder–support vector machine–grasshopper optimization for intrusion detection system. International Journal of Intelligent Engineering and Systems, 15(4), 406-414.

[22] Khan, M. A. (2021). HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. Processes, 9(5), 834.

[23] Ghafir, I., Kyriakopoulos, K. G., Lambotharan, S., Aparicio-Navarro, F. J., Assadhan, B., Binsalleeh, H., & Diab, D. M. (2019). Hidden Markov models and alert correlations for the prediction of advanced persistent threats. IEEE Access, 7, 99508-99520.

[24] Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. Future Generation Computer Systems, 89, 349-359.

[25] Giura, P., & Wang, W. (2012, December). A context-based detection framework for advanced persistent threats. In 2012 International Conference on Cyber Security (pp. 69-74). IEEE.

[26] Brogi, G., & Tong, V. V. T. (2016, November). Terminaptor: Highlighting advanced persistent threats through information flow tracking. In 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.

[27] AMINU, M., AKINSANYA, A., OYEDOKUN, O., & TOSIN, O. (2024). A Review of Advanced Cyber Threat Detection Techniques in Critical Infrastructure: Evolution, Current State, and Future Directions.

[28] Ghafir, I., & Prenosil, V. (2016). Proposed approach for targeted attacks detection. In Advanced Computer and Communication Engineering Technology: Proceedings of ICOCOE 2015 (pp. 73-80). Springer International Publishing.

[29] Mishra, R., Kumar, K., Mehta, S. N., & Chadhuary, N. (2024, March). Exploring the Effects of Block Chain-Based Security Systems on Cyber Security. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 687-692). IEEE.

[30] Mishra, R., Tripathi, P., & Kumar, N. (2024). Application of Emotional Intelligence in Improvement of Human-Robot Collaboration. In Human-Machine Collaboration and Emotional Intelligence in Industry 5.0 (pp. 251-267). IGI Global.



Authorized licensed use limited to: RNS Institute of Technology. Downloaded on March 07,2025 at 13:51:07 UTC from IEEE Xplore. Restrictions apply.