DOI: 10.2507/35th.daaam.proceedings.038

MACHINE LEARNING FOR THREAT DETECTION IN SOCS

Ema Josipovic, Damir Regvart*, Ana Kapulica & Robert Kopal

This Publication has to be referred as: Josipovic, E[ma]; Regvart, D[amir]; Kapulica, A[na] & Kopal, R[obert] (2024). Machine Learning for Threat Detection in SOCs, Proceedings of the 35th DAAAM International Symposium, pp.0279-0285, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-44-0, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/35th.daaam.proceedings.038

Abstract

This paper explores the integration of Machine Learning (ML) algorithms within Security Operations Centres (SOCs) for enhanced cyber threat detection. It examines the effectiveness of various ML algorithms, such as Random Forest and SVM, in identifying and mitigating cyber threats. The paper delves into the inherent challenges associated with ML in cybersecurity, including vulnerabilities to adversarial attacks and issues of overfitting. Strategies to overcome these challenges are discussed, highlighting the importance of advanced data handling and the necessity of human expertise alongside ML. The paper concludes by emphasizing the transformative potential of ML in cybersecurity, advocating for continuous innovation and ethical considerations in its application.

Keywords: Machine Learning; Cybersecurity; Security Operations Centres; Threat detection; Random Forest

1. Introduction

Security operations centers (SOCs) are teams of IT security specialists responsible for continuously monitoring an organization's entire IT infrastructure. They promptly detect and respond to cybersecurity events, ensuring swift and efficient action [1]. In the absence of immediate threats, SOCs analyze threat data to develop new and improved security solutions, enhancing the organization's overall security posture. SOC duties and activities can be broadly categorized into three areas:

- Preparation, planning, and prevention,
- Monitoring, detection, and response,
- Recovery, refinement, and compliance.

SOCs perform regular maintenance and preparation tasks, such as updating firewalls, applying software patches, and backing up systems. They also develop an incident response plan detailing roles, tasks, and response metrics. Regular tests, including penetration and vulnerability assessments, help SOCs identify potential risks and costs. Staying informed about the latest security threats and solutions ensures business continuity during a cyberattack. In addition, SOCs are responsible for continuous monitoring, identification, and response for networks, servers, system software, applications, computing devices, cloud workloads, and system software.

Security information and event management (SIEM) is the primary technology used for this purpose [2], gathering real-time alerts from network hardware and software, analyzing them, and detecting potential threats. Log management is a crucial monitoring aspect, highlighting anomalies that indicate suspicious activity. When a threat or incident occurs, the SOC mitigates damage, which may involve root cause analysis, root cause investigation, isolating compromised areas, exiting or reversing affected applications, deleting files, and deploying antivirus or anti-malware software.

The SOC is responsible for recovery, improvement, and compliance management after an incident. It mitigates risks, repairs damaged assets and incorporates new intelligence to patch vulnerabilities and update procedures. Additionally, it ensures compliance with data privacy laws such as GDPR, CCPA, PCI DSS, and HIPAA. Post-incident, the SOC ensures incident data is preserved for auditing and evidence and informs users, regulators, law enforcement, and other relevant parties.

The SOC's structure generally includes a SOC Manager, Security Engineers, Security Analysts, and Threat Hunters. The SOC Manager oversees all security operations and reports to the Chief Information Security Officer. Security Engineers design the company's security architecture, while Security Analysts are the first responders to cybersecurity threats or incidents. Threat Hunters specialize in identifying and neutralizing advanced threats that evade automated defenses. Depending on the organization's size and industry, other specialists may be part of the SOC team. Larger organizations may employ a Director of Incident Response to coordinate and manage incident response efforts. Additionally, some SOCs have Forensic Investigators who specialize in recovering data clues from compromised devices during cybersecurity incidents.

2. Overview of Integrating Machine Learning for Threat Detection

Before exploring the use of Machine Learning for threat detection in SOCs, it's essential to define it. Machine Learning, a branch of Computer Science and Artificial Intelligence, employs data and algorithms to mimic human learning processes and improve accuracy over time (IBM, 2024b). Algorithms are trained using statistical techniques to make predictions or classifications and uncover significant information in data mining projects. These insights are then used to inform business and application decisions, ideally positively impacting key growth metrics.

Despite the existing clever marketing messages and some reporting, Machine learning is not a security cure-all. Still, it can substantially support security and IT organizations [3]. While Machine Learning has a long way to go before it can detect threats without human interaction, it can undertake various tasks to improve cybersecurity. Some examples of specific areas where machine learning may be used to simplify and enhance cybersecurity tasks include Phishing and spam filtering, Forensic analysis, Incident response and risk management, penetration testing, and threat modeling and prevention. In the case of Phishing and spam filtering, ML may, by using predefined parameters, assist in accurately classifying internal data, spam, and malicious actions. In Forensic analysis, ML can, by using clustering, assist in obtaining information about the assault strategy and targets. Clustering collects and groups data, making it easier for the team to piece together the elements of the attack. Furthermore, the software learns from the actions taken during various incidents through ML for incident response and risk management. Machine learning can identify actions for incident response and risk mitigation based on patterns and relationships. In the case of penetration testing, programs can generate inputs to test systems for vulnerabilities like a penetration tester searching for flaws. Finally, in Threat modeling and prevention, Machine learning gathers and evaluates data to forecast fraudulent activity. This aids security teams in spotting dangers before they develop into costly and significant data breaches or thefts.

Applying Machine Learning algorithms can streamline and enhance the efficiency of numerous cybersecurity tasks. This technology can significantly reduce workload, decrease human error, and improve decision-making processes. Additionally, these adaptive strategies and tactics can be tailored to fit the specific needs of a business or organization, providing a customized approach to cybersecurity that maximizes effectiveness and aligns with organizational goals. The flexibility and precision of Machine Learning make it a powerful tool in the ongoing effort to protect digital assets and maintain robust security postures.

3. Machine Learning Algorithms for Threat Detection

Threat detection in cybersecurity, including in Security Operations Centres (SOCs), involves using various machine learning algorithms [4]. The choice of which algorithm to use depends on multiple factors, including the specific use case, available data, and the nature of the threats being dealt with. There is also the option of a hybrid approach, which includes combining multiple algorithms, usually done to enhance the overall threat detection capabilities of the Machine Learning model.

The most used algorithms, due to their effectiveness in identifying patterns, anomalies, and potential threats, described by this paper use cases are:

- Supervised Learning Algorithms
- Unsupervised Learning Algorithms
- Reinforcement Learning Algorithms

3.1. Supervised Learning Algorithms

Supervised learning algorithms are machine learning algorithms that learn from labeled training data to make predictions or classifications. In supervised learning, each training example consists of an input object (typically a vector) and a desired output value (also called the supervisory signal). The algorithm learns to map inputs to the correct output based on this labeled data, allowing it to predict the production of new, unseen inputs.

Random Forest is an ensemble learning method that can be used for classification tasks in threat detection. It combines multiple decision trees to improve the accuracy and robustness of the model. An example use case could be as follows: Random Forest can analyze web traffic and classify URLs as benign or malicious. By training the model on a labeled dataset of URLs, the algorithm learns patterns indicative of malicious links. In a SOC, this can help identify and block phishing attempts or links leading to malicious sites, enhancing overall web security.

Support Vector Machines (SVM) are practical algorithms for binary and multi-class classification problems. They work well for identifying patterns in data, making them useful for detecting anomalies or malicious activities. An example use case could be as follows: SVMs can be applied to user behavior analytics to identify potential insider threats. By training on historical data, the SVM model learns standard patterns of user activities. The SVM can raise alerts for further investigation when deviations or anomalies occur, such as unusual file access or login behavior.

Naive Bayes is a probabilistic classifier based on Bayes' theorem. It's simple and efficient, making it suitable for real-time threat detection applications. An example use case could be Email Spam Filtering since Naive Bayes is well-suited for email security in SOCs. By analyzing the content and metadata of emails, the algorithm can classify messages as either spam or legitimate. This helps automatically filter out malicious emails and reduce the risk of phishing attacks.

3.2. Unsupervised Learning Algorithms

Unsupervised learning algorithms are machine learning algorithms that work with unlabelled data. Unlike supervised learning, which learns from labeled input-output pairs, unsupervised learning identifies patterns and structures in the data without predefined labels. These algorithms are beneficial for discovering hidden structures, clustering similar data points, and reducing data dimensionality.

K-means clustering is a widely used clustering algorithm that identifies patterns and groups similar data points. It can be employed for anomaly detection by identifying clusters that deviate from the norm. An example use case could be Network Intrusion Detection. It can be applied to network traffic data to identify clusters of normal behavior. Any deviations from these clusters may indicate a potential network intrusion. SOC analysts can then investigate these anomalies to detect and respond to security incidents.

Isolation Forest is an ensemble method for anomaly detection. It builds a tree structure to isolate anomalies more efficiently than traditional methods. An example use case could be Anomaly Detection in System Logs. By creating a model on standard log patterns, the algorithm can efficiently isolate and flag abnormal log entries, which may indicate unauthorized access or other security incidents.

Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is a density-based clustering algorithm that can identify clusters of varying shapes and effectively detect outliers, which may represent security threats. One example of its use is Identifying Port Scans. The algorithm can analyze network traffic and identify patterns associated with port scanning activities. Unusual clustering of connections to multiple ports from a single source IP address may suggest a potential reconnaissance attempt, triggering an alert for further investigation.

3.3. Reinforcement Learning Algorithms

Reinforcement learning (RL) algorithms are a category of machine learning algorithms that enable an agent to learn how to make decisions by performing actions in an environment to maximize some notion of cumulative reward. Unlike supervised learning, where the model learns from a dataset of labeled examples, reinforcement learning involves learning from actions' consequences rather than direct instruction.

Q-learning is a model-free reinforcement learning algorithm. In cybersecurity, it can train an agent for adaptive firewall rule management. The agent learns to adjust firewall configurations based on evolving threat landscapes, optimizing for security and performance in real-time.

Deep Q Networks (DQN) is an extension of Q-Learning that uses deep neural networks to approximate the Q-function. It can handle more complex and high-dimensional state spaces, making it suitable for cybersecurity applications. An example use case is using DQN for dynamic threat response by training an agent to decide on incident response actions. The model learns optimal strategies for mitigating specific threats, enabling automated and intelligent responses to security incidents.

Multi-Armed Bandits can be used when decisions must be made in uncertain environments. It's relevant for dynamically adapting defense strategies based on evolving threats during incident response. By continuously learning from the effectiveness of different response strategies, the algorithm optimizes resource allocation to maximize the SOC's ability to mitigate and respond to security incidents effectively.

4. Effectiveness of Machine Learning in SOCs - Strengths and Weaknesses

Machine Learning algorithms have demonstrated their proficiency in identifying and hindering cyber threats, capitalizing on their capacity to adapt to changing and emerging patterns of attacks. This section explores the varied ML algorithms and their impact on cyber security, highlighting their adaptability and learning capabilities. In a series of studies, different Machine Learning algorithms were assessed for their effectiveness in cyber-attack detection [5]. Random Forests and Logistic Regression were most efficient in phishing attack detection, with accuracies of 98.64% and 98.59%, respectively. They demonstrated Random Forests [6] superiority in malware detection, achieving a 99.63% accuracy. Random Forests' effectiveness in DDoS and network intrusion detection, respectively. These studies [7][8] collectively underscore the high efficacy of ML algorithms, especially Random Forests shown in Table 1, in combating various cyber threats.

Cyber-Attack Type	Accuracy of Random Forest
Malware Attacks	99,68%
DDoS Attacks	99,48%
Network Intrusion Attacks	99,31%
E-mail SPAM	98,72%

Table 1. Effectiveness of Random Forest in Detecting Different Types of Cyber Attacks

Machine Learning Algorithm:	Advantage:	Disadvantage:
Decision Trees	Easy to interpret and explain, fast training time	Can overfit on training data
Random Forest	Can handle large datasets, less prone to overfitting than decision trees	It can be computationally expensive
Native Bayes	Simple and fast, it requires less training.	Assumes independence between features, which may not be accurate in some cases
Logistical Regression	Easy to interpret and explain, can handle non-linear relationships between features	It may not perform well when features have complex interactions, or the decision boundary is non-linear.
Support Vector Machine (SVM)	Effective for high-dimensional features, can handle non-linear decision boundaries	It can be computationally expensive.
Neural Networks	Can learn complex relationships between features and can handle large datasets.	Requires a lot of training data, prone to overfitting
Clustering	It can detect anomalies in data, which helps identify new types of attacks.	It can be computationally expensive and challenging to interpret.
Reinforcement Learning	Can adapt to changing environments, useful for detection of dynamic attacks	Requires a lot of training data, can be computationally expensive

Table 2. Advantages and Disadvantages of Machine Learning Algorithms for Cyber-Attack Detection and Prevention

As is visible from Table 2, in cyber-attack detection and prevention, various Machine Learning algorithms offer a balance of strengths and weaknesses. Supervised learning algorithms, known for their efficacy in recognizing established threat patterns, are highly accurate due to their reliance on pre-labeled datasets. However, their dependency on prior knowledge makes them less effective against novel threats. On the other hand, unsupervised learning thrives in detecting these unknown threats by identifying anomalies without needing labeled data, although it may yield higher false-positive rates. Moreover, reinforcement learning stands out for its adaptability and continuous learning from the environment, offering a dynamic approach to evolving cyber threats. However, this comes at the cost of increased complexity and computational resources. More specifically, it can be said that Decision Trees are lauded for their quick training and simplicity but are vulnerable to overfitting. Random Forests are robust against overfitting and capable of handling complex data, yet computationally demanding.

Naive Bayes is efficient and requires less data but may falter with interdependent features. Logistic Regression works well with non-linear relationships but struggles with complex interactions. SVMs excel in high-dimensional spaces but are sensitive to kernel functions. Neural Networks can model intricate relationships and manage voluminous data but tend to overfit. Clustering algorithms are adept at anomaly detection but can be complex and resource intensive. It can be concluded that each algorithm's applicability depends on the specific requirements and limitations of the cybersecurity task at hand. Since each machine learning algorithm offers distinct advantages and unique challenges, careful evaluation is needed to determine the most suitable approach for a specific SOC environment and security threat.

5. Challenges in Training Machine Learning Models within SOC

Even though machine learning algorithms have succeeded in identifying and stopping cyberattacks, they have some drawbacks [9]. A few of machine learning's shortcomings in cyber security will be discussed in this paragraph. The susceptibility of machine learning to adversarial attacks is one of its drawbacks. Adversarial attacks are vicious and purposeful attempts to cause disturbances in the input data to trick Machine Learning algorithms. Machine learning algorithms may misclassify data because of adversarial attacks, which could result in successful cyberattacks. The vulnerability of machine learning to overfitting is another drawback. When a machine learning system is trained on a small amount of data, it becomes overfitted and has poor generalization to new data. Overfitting can result in false positives and negatives in the context of cyber security, leading to missed threats and resource loss. Overfitting may happen when machine learning algorithms are used for intrusion detection [10]. Another constraint on machine learning algorithms is the quantity and quality of training data. A machine learning system might not be able to reliably identify or stop cyberattacks if the training data is biased or lacking. Additionally, because the algorithm might need to correctly categorize data that differs from the training set, a lack of diversity in the training data can result in poor generalization. Machine learning algorithms may be computationally costly and need much memory and processing capacity. This may restrict its applicability and scalability, especially for resource-constrained organizations. Finally, the application of ML in cybersecurity raises ethical and privacy issues [11]. It's an enormous task to balance user privacy and security, and it is riddled with moral and legal issues. Ensuring the ethical use of technology requires strict adherence to data governance principles and robust data protection measures to preserve user confidence and comply with legal requirements. Machine learning algorithms have shown considerable promise in detecting and preventing cyberattacks; however, they have limitations. When utilizing machine learning in cybersecurity, it is crucial to consider several factors, including computational complexity, overfitting, the quality and diversity of training data, and susceptibility to adversarial attacks.

6. Strategies to Address the Challenges

A comprehensive strategy is essential to addressing the challenges encountered by Machine Learning in cybersecurity [12]. Effective data management is central to robust model training. This includes employing sophisticated techniques for data acquisition, preprocessing, and feature extraction, enhancing data quality and model performance. Simultaneously, optimizing algorithmic efficiency can be achieved through parallel computing, enabling the scaling of models to handle large and diverse datasets. Continuous model maintenance and adaptation are tackled through transfer learning and ensemble methods, bolstering generalization and resilience against adversarial attacks. Integrating human expertise with Machine Learning ensures a more nuanced approach to threat detection, as humans can provide insights that pure Machine Learning may overlook. Ensuring model interpretability and explainability is equally crucial; transparent models foster trust and facilitate easier management. Upholding legal and ethical standards is imperative, guaranteeing user trust through rigorous data protection and privacy measures. These strategies collectively establish a robust framework for overcoming the inherent limitations of Machine Learning in cybersecurity.

Incorporating Machine Learning into cybersecurity demands significant investment in advanced solutions and expert talent [13]. Equipping experts with AI tools position them better to keep pace with evolving cyber threats. Addressing AI biases is critical; cybersecurity AI must be trained on diverse datasets to ensure fairness and prevent skewed outcomes. Acknowledging vulnerabilities in AI, such as susceptibility to hacker exploitation, is paramount. AI should be viewed as a complementary tool rather than a substitute for human specialists, emphasizing continuous development and establishing legal frameworks to safeguard against AI misuse in cyber activities. This multifaceted approach strengthens AI's role in cybersecurity, balancing innovation with vigilance. Continuous research and development activities are necessary to address these difficulties and improve the robustness, resilience, and efficacy of ML-based cybersecurity systems [14]. Some possible ways to address the challenges include:

- Creating robust machine learning algorithms and resilient structures,
- Improving data gathering and labeling strategies,
- Adding explainability techniques and modifying models in response to evolving risks via ongoing monitoring and learning

7. Real-world Applications and Future Research

Machine learning has many applications for enhancing cybersecurity within SOCs [15]. This paragraph highlights five real-life examples for future research activity.

Firstly, **network traffic analysis** relies on machine learning algorithms to identify and mitigate DDoS attacks, forecast future threats by analyzing traffic volume, and detect botnet activities. For instance, algorithms can swiftly identify spikes in traffic during a DDoS attack, prompting timely action from relevant authorities within the organization. Additionally, these algorithms can pinpoint the attack vector or type of assault, enabling SOC teams to defend against similar cyber threats proactively. Moreover, machine learning techniques in network traffic analysis can detect and counteract bots or botnet activities, thus protecting servers from malicious actors seeking to exploit them.

In **endpoint security**, machine learning complements anti-virus software by detecting and categorizing various types of malware, bolstering defenses against emerging digital threats. Protecting endpoints from viruses and malware is paramount, and machine learning algorithms play a crucial role in uncovering hidden cyber dangers, thereby fortifying the efficacy of firewalls and anti-virus software. Furthermore, machine learning algorithms can classify incoming malicious packages as spyware, ransomware, or malware, empowering SOC teams to prioritize and mitigate potential online threats effectively. ML-assisted endpoint protection can swiftly identify anomalies at endpoints, alert authorities, and expedite threat detection processes.

Machine learning plays a vital role in **enhancing application security** as well. Web Application Firewalls and other application security solutions leverage machine learning to shield servers and systems from cyberattacks targeting the application layer of the OSI model. ML-based solutions, for instance, can be engineered to detect anomalies in HTTP requests and issue alerts in case of an attack. They can also be trained to recognize attack vectors and classify various types of assaults, such as SQL injection and XSS attacks. SOC teams can bolster their cyber protection infrastructure by leveraging insights from these algorithms.

Authentication security also benefits from machine learning. Various authentication security measures, including two-factor authentication, CAPTCHA, and biometric methods like fingerprint and facial recognition, aim to thwart account takeovers and online identity fraud. Facial and fingerprint recognition software employs ML algorithms to provide additional security to computers and mobile devices. Machine learning in authentication security utilizes additional techniques to thwart account takeover attempts better. Adversaries often employ brute force or credential-stuffing techniques to access accounts, potentially leading to organization network breaches. Machine learning methods can identify and thwart such attacks, with trained systems capable of detecting and intercepting the trial-and-error phase of these attacks.

Furthermore, machine learning significantly contributes to **attack surface management** by continuously monitoring organizational vulnerabilities. This support enables SOC teams to uphold a robust security posture. Given the continued expansion of the digital attack surface for significant firms, managing and monitoring an organization's attack surface can be burdensome for SOC teams. Machine learning offers a solution by alleviating the workload on SOC teams and providing error-free monitoring and management capabilities.

8. Conclusion

This paper demonstrates the crucial role of Machine Learning (ML) in bolstering cybersecurity within Security Operations Centres (SOCs). It underscores the benefits of various ML algorithms, such as Random Forest and SVM, in identifying and addressing cyber threats while acknowledging their limitations, including susceptibility to adversarial attacks and overfitting. Furthermore, it proposes comprehensive strategies to overcome these challenges, emphasizing the significance of advanced data management, ongoing model refinement, and the fusion of human expertise. This amalgamation of human and artificial intelligence enhances threat detection and lays the foundation for a more resilient and sophisticated cybersecurity framework. The paper highlights the intersection of ML and human intelligence in SOCs as indicative of the evolving cybersecurity landscape, emphasizing the imperative of continuous innovation and ethical considerations in this dynamic domain.

9. References

[1] https://www.ibm.com/topics/security-operations-center, (2024). IBM: What is a security operations center (SOC)?, Accessed on: 2024-01-08

[2] Suskalo, D., Moric, Z., Redzepagic, J., & Regvart, D. (2023). Comparative Analysis of IBM Qradar and Wazuh for Security Information and Event Management. In DAAAM Proceedings (pp. 0096–0102). DAAAM International Vienna, DOI: 10.2507/34th.daaam.proceedings.014

[3] Nemelka, K. (2023) Ki und ML in der cybersecurity, Security. Available from: https://www.security-insider.de/ki-und-ml-in-der-cybersecurity-a-5a3830cdaf3d26e192de9066e37c4234/ , Accessed: 2024-01-08

[4] Chukhnov, A.P. & Ivanov, Y.S. (2021). "Algorithms for Detecting and Preventing Attacks on Machine Learning Models in Cyber-Security Problems", Journal of Physics: Conference Series, Vol. 2096, Issue 1, p. 012099, DOI 10.1088/1742-6596/2096/1/012099

[5] Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. A. (2020). "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review", In Procedia Computer Science, Vol. 171, pp. 1251–1260, DOI: 10.1016/j.procs.2020.04.133
[6] Geetha, R., & Thilagam, T. (2020). "A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security", In Archives of Computational Methods in Engineering, Vol. 28, Issue 4, pp. 2861–2879, DOI: 10.1007/s11831-020-09478-2
[7] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A. & Marchetti, M. (2018). "On the effectiveness of machine and deep learning for cyber security", In 2018 10th International Conference on Cyber Conflict (CyCon), ISBN:978-9-9499-9043-6, ISSN: 2325-5374, DOI: 10.23919/cycon.2018.8405026
[8] Sreekanth, D. et al. (2023) 'An Analysis Of The Effectiveness Of Machine Learning Algorithms In Detecting And Preventing Cyber-Attacks', Analysis of the Effectiveness of Machine Learning Algorithms in Detecting and Preventing Cyber-Attacks [Preprint].
[9] Bharadiya, J. (2023). "Machine Learning in Cybersecurity: Techniques and Challenges", In European Journal of Technology, Vol. 7, Issue 2, pp. 1–14, DOI:10.47672/ejt.1486
[10] Bagaa, M., Taleb, T., Bernabe, J. B., & Skarmeta, A. (2020). "A Machine Learning Security Framework for IoT Systems". In IEEE Access, Vol. 8, pp. 114066–114077, ISSN: 2169-3536, DOI: 10.1109/access.2020.2996214
[11] Sabo, J. (2023) Machine learning and AI in SOC: Enhancing threat detection, LinkedIn. Available at: https://www.linkedin.com/pulse/machine-learning-ai-soc-enhancing-threat-detection-john-sabo-9syqc/, Accessed: 2024-01-05
[12] Intone Networks (2023) Challenges & Solutions for machine learning in Cybersecurity, Intone Networks. Available at: https://intone.com/challenges-and-solutions-in-implementing-machine-learning-for-cybersecurity/, Accessed on: 2024-01-08
[13] Cybernetic Search (2023) Assessing the benefits and challenges of AI in cyber security, Cyber Security and Software Engineering Recruitment. Available at: https://www.cyberneticsearch.com/blog/assessing-the-benefits-and-challenges-of-ai-in-cyber-security/ (Accessed: 05 January 2024).
[14] Bharadiya, J. (2023). "Machine Learning in Cybersecurity: Techniques and Challenges", In European Journal of Technology, Vol. 7, Issue 2, pp. 1–14, DOI: 10.47672/ejt.1486
[15] SOCRadar (2022). "Real-life examples of machine learning in Cybersecurity", In SOCRadar Cyber Intelligence Inc. Available at: https://socradar.io/real-life-examples-of-machine-learning-in-cybersecurity/, Accessed on: 2024-01-05