Proceedings of the 2nd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/73/20240409

Early detection and mitigation of cyber attacks with machine learning and artificial intelligence

Encheng Liu

Heilongjiang University of Science and Technology, No. 2468 Puyuan Road, Songbei District, Harbin City, Heilongjiang Province, China

wyyxlec@163.com

Abstract. This research article explores the influence of leveraging machine learning algorithms (ML) and artificial intelligence (AI) in the early detection and mitigation of cyber attacks. With the rise of cybercriminal activities, traditional cybersecurity measures have proven inadequate. This study reviews the various AI and ML techniques, such as anomaly and cyber intelligence, which can be used in detecting cyberattacks before they occur. A case study on IBM security illustrates the practical implications and outcome of implementing machine learning and artificial intelligence in cybersecurity.

Keywords: Cyber security, Machine learning, Cyber-attack, Artificial intelligence.

1. Introduction

The developing impact of telecommunication networks, as well as the internet metaphor, have contributed to the rise of unprecedented cybercriminal activities [1]. The vehicular networks across various industries have posed risks to the users to cybersecurity threats. The stealthy cyberattacks growing threats on the financial sectors, government organizations, and data centers have represented major challenges to disseminating information [2; 3]. Complex cyberattacks usually rely on malicious software or malware to exfiltrate sensitive data, identity theft, cyber espionage, and financial threats. Initially, the cyber-attacks were being addressed through creating data backups and encrypting sensitive information from being accessed by third parties [4]; however, these strategies were seen to be incompetent in early detection and mitigation of the cyber threats. While researchers have explored topics on the traditional methods of encrypting, this paper explores the benefits and challenges of using ML and AI in the early detection as well as mitigation of cyber attacks. This discussion will explore how machine learning and artificial intelligence can be leveraged to enhance early detection and mitigation of cyber threats.

2. Background

The term cyber threats refers to malicious activities in the digital world that compromise the availability, integrity, and confidentiality of the networks, computer systems, and data [5]. These threats encompass a wider range of actions, such as hacking attempts, phishing attacks, malware infections, and other unauthorized actions that may compromise the security of digital assets. Cyber threats usually pose significant risks to the targets, requiring constant vigilance and proactive measures to mitigate their

DOI: 10.54254/2755-2721/73/20240409

occurrence. With the technological advancements, artificial intelligence and machine learning have turned out to be the most effective strategies for reducing cyber-attack chances. Artificial intelligence is explored in computer science and technology, which usually focuses on creating systems and machines responsible for performing tasks [6]. Machine learning is also a part of artificial intelligence focusing on the algorithms development and models that enable a computer to reduce time for data processing. In cybersecurity, techniques and approaches, cyber security analytics, digital forensics, and cyber threat intelligence have assisted in detecting, analyzing, and neutralizing cyber threats before an attack occurs [7]. By leveraging these technologies, individuals and organizations can get effective and resilient cybersecurity solutions to address the modern malware detention as well as analysis in real-time automation.

3. Literature Review

Artificial intelligence and machine learning in cybersecurity have gained insights from various researchers and computer experts exploring its impacts on this sector. This literature review provides what the researchers have found on various artificial intelligence and machine use, its benefits, and its challenges in the cybersecurity sector.

a)Artificial Intelligence and Machine Learning Tools used in Cybersecurity

Provided there is cyberattack surfacing in the digital world providing cyber threats, there are various artificial intelligence and machine learning that have been implemented, which include:

3.1. Anomaly Detection

Studies show anomaly detection as an example of machine learning and artificial intelligence models trained to establish the baseline for normal network and user behavior. A study conducted by Blázquez-García et al. found this model examines the specific data points and detects rare occurrences that may seem to be suspicious [8]. Anomaly detection analyzes the data such as the login patterns, network traffic, and data access. When the deviation is made from the baseline, it indicates that there is a potential cyberattack. For example, whenever an employee who usually accesses a set of files suddenly attempts to access sensitive files, it can be flagged for investigation.

3.2. UEBA

The literature on UEBA, or User and Entity Behavior Analytics, explains it as a cybersecurity solution utilizing machine learning and algorithms in detecting the anomalies in the behaviors of both the users in the routers and corporate network [9; 10]. Machine learning builds user profiles by monitoring user activities, resource usage, and accessing patterns. These models can then detect deviations from these profiles, such as a profile attempting unauthorized access, which might mean that there are compromised accounts or insider threats.

3.3. Cyber Security Analytics

The research on cyber security analytics has explored it as a proactive approach in the cybersecurity field known to use the collection of data, analysis, relationship, and aggregation capabilities in performing significant security functions in analyzing, neutralizing, and detecting threats and vulnerabilities whenever they occur [11]. This research has shown that the CSA is used to detect, prevent, and mitigate modern and advanced malware, weak credentials, unpatched vulnerabilities, DDoS cyberattacks, social engineering, and advanced persistent threats, which are key areas of cyber threats.

3.4. Cyber Threat Intelligence

Literature on cyber threat intelligence categorizes it as an intelligence technique used in the detection of attacks before they happen. This method is known in collecting and organizing all the information that are related to cyber-attacks in the cyberspace to help in drawing a cyber-attackers cartography and highlighting the trends [12; 13]. This literature shows that CTI is gathers data on potential attackers and analyzing and processing the information to better understand that threat. This example of cyberattacks

DOI: 10.54254/2755-2721/73/20240409

is usually split into two main areas, which include tactical, operational, and strategic attack intelligence. CTI usually operates on a life cycle, with stages such as processing, collection, analysis, feedback, direction, as well as dissemination.

3.5. Intrusion Prevention/Detection

Scholars state that intrusion detection is a system known to monitor the network continuously and identifies any potential incident of cyberattack that may occur [14]. The system usually records information related to the reports, resolves incidents, and logs them to security administrators. Research shows that intrusion detection analyzes the network traffic for patterns or anomalies consistent with the known attack technique. When suspicious activities are detected, the systems automatically block the traffic and take preventive measures to mitigate the potential threats.

3.6. Leveraging ML and AI in Cybersecurity

Researchers have explored various benefits of applying ML and AI in cybersecurity. Here are some of these benefits:

3.7. Early Detection of Cyber Threats

Literature on the positive impacts of ML and AI in cyber-attacks explains that early cyber-attack detection is among the main benefits experienced. Artificial intelligence-driven systems operate at a machine speed, which allows them to respond to threats in real-time [1]. The security systems installed in machine learning analyze massive volumes of data, spot unusual activity, and find the trends that can show a cyberattack. For example, artificial intelligence and machine learning algorithms can select the hacker trying to enter in a bank system from an unidentified place and then informs the information technology team before it is done.

3.8. Improved Threat Response

Research has also shown that improved threat responses are an advantage organizations enjoy from using artificial intelligence and machine learning. With AI and ML, security systems automatically blocking or quarantining malicious activity, which reduces the response time that the security team's mind needs [7]. Such models and tools, such as anomaly detection, can even identify complex patterns indicating cyber threats. This capability makes these models subtle, sophisticated attacks that the traditional security systems may not notice.

3.9. Reduced the False Positives

Literature shows that the false context in cybersecurity is reduced through artificial intelligence and machine learning. False positives refer to the alerts and warnings generated by security systems that may incorrectly identify benign or legitimate activities as potential threats [15]. These false alarms may cause the organization to overwhelm the security teams with alerts, making them find it challenging to differentiate between non-threatening events and real threats. The literature on artificial intelligence and machine learning in cybersecurity states that false positives can waste organizations' valuable time and resources and alert fatigue.

3.10. Automated Security Operations

Research has also shown that machine learning and artificial intelligence benefit organizations by providing automated security operations limited to human error and workload for the security teams [9]. The security systems used in artificial intelligence and machine learning can automatically recognize and prioritize security incidents, take corrective actions, and send notifications with one expert or none. In the traditional methods such as encryption, many security operators were needed to always countercheck the documents and send notifications. The security operators might also be among those attempting to attack the organization's database, who might also be detected by artificial intelligence and machine learning models.

DOI: 10.54254/2755-2721/73/20240409

3.11. Difficulties of Using Machine Learning and Artificial Intelligence

Even though researchers find the use of AI and ML is effective in detecting and mitigating cyber-attacks, literature also shows that there are difficulties in using these systems, which include:

3.12. Complexity and Uncertainty

The data collected in cyber security can be difficult, varied, and vast in interpreting, making it difficult for algorithms in processing, analyzing, and detecting any potential threat that may occur [3]. The cyber security data uses programming languages that differ from the human language, creating complexity in accessing the threats. Also, cybercriminals are introducing new procedures, and tactics to help in evading security measures, creating more complexity to the data. Many artificial intelligence and machine learning, especially deep learning models, are considered black boxes since they are challenging to understand how to arrive at the decisions. Consequently, machine learning and artificial intelligence may not manage to identify all the potential security threats, hence exposing companies to cyber-attacks.

3.13. Limited Human Oversight

Research on the challenges of using ML and AI in cybersecurity has it that it is potentially limited to human oversight. Even though artificial intelligence as well as machine learning can analyze and process data faster, they may sometimes make inaccurate decisions on an independent basis but might require experts. This means that human oversight is important on ensuring that false negatives and positive are flagged and algorithms work as expected. Nevertheless, the high volume of cybersecurity data may be challenging for humans to keep up with the accuracy and speed of machine learning and artificial intelligence.

3.14. Cybersecurity Skills Gap

Literature also shows that there is a gap with the cybersecurity experiences. Although artificial intelligence and ML can help to automate some of the cybersecurity jobs, qualified individuals are also needed who understand and act on these algorithms [4]. Many organizations are still struggling to get an expert or qualified cybersecurity professional who can work with artificial intelligence and ML to reduce cyberattacks. Also, the cost of training the personnel for implementing and maintaining machine learning and artificial intelligence can be challenging for small organizations.

4. Case Study

This conference paper leveraged a case study on the use of AI and ML in IBM Security Company. Specifically, the objective of this case study was to understand the impacts artificial and machine learning have in the reduction of cyber-attacks.

Implementation Process

This study was conducted at IBM Security Company through a qualitative approach. This method effectively collected in-depth insights from the participants on how their companies use machine learning and artificial intelligence to safeguard other organizations from cyber-attacks. IBM Security Company known in providing an enterprise for cyber-attack solutions in helping thrive in the cyberattacks and uncertainty face. This company helps protect the business with an advanced as well as integrated enterprise cybersecurity solutions portfolio, which are then infused with artificial intelligence. This company was chosen since it is among those who have already implemented artificial intelligence and machine learning in cyber security and have shown significant impacts.

Data Collection

A total of 10 participants were chosen to participate in explaining how machine learning and artificial intelligence can be leveraged in detecting and mitigating cyber-attacks. The participants engaged in interviews of 20 minutes, each explaining how their organization helps ensure that other companies are protected from cyber-attacks. Only those employees working in either of the IBM company branches were selected. The interviews were recorded and later transcribed, and then the data set was analyzed.

DOI: 10.54254/2755-2721/73/20240409

5. Results and Discussion

The results of the interviews show that artificial intelligence and machine learning have contributed to positive solutions such as:

i.Top solutions: these consist of threat intelligence solutions, cloud security solutions, ransomware solutions, and IAM solutions. In threat intelligence solutions, the participants note that they have outsmarted attacks using a connected modernized security suite, which helps in threat detection and response solutions to unify the security analyst experience. Ransomware protection solutions through detecting and responding to the ransomware, identifying the vulnerabilities, and minimizing the impacts if they happen.

ii.Cybersecurity solutions: these solutions include data security and protection solutions, unified endpoint management solutions, AI cybersecurity solutions, and mobile security solutions. Specifically, AI cybersecurity solutions provide transformative, AI-powered solutions for accelerating threat detection and protecting user identity while also keeping the security teams in the loop. Data security and protection solutions provided two sides of the cybersecurity attack. These solutions have complex compliance regulations, which include CCPA, PCI, SOX, DORA, and GDPR, which prevent unauthorized individuals from accessing the user's and customers' sensitive information.

The results from the interviews also show that the company experiences various challenges from using artificial intelligence and machine learning in cyber security, which include:

i.Data quality and quantity: machine learning and artificial intelligence models rely more on vast amounts of data for detecting threats. Ensuring the quality, relevance, and accuracy of this data is most challenging.

ii.Adversarial attacks: cyber attackers have also learned ways of attacking artificial intelligence and machine learning through adversarial techniques. This usually consists of the manipulation of input data to evade detection.

6. Conclusion

In summary, the use of artificial intelligence and machine learning in cybersecurity, as exemplified by IBM Security, presents significant advantages in early threat detection, improved response, reduced false positives, and automated security operations. These technologies empower organizations to proactively address modern cyber threats. However, challenges such as data complexity, the need for human oversight, and the cybersecurity skills gap must be acknowledged. As the cyber threat landscape evolves, it is essential to strike a balance between harnessing the potential of AI and ML and addressing these challenges to enhance cybersecurity resilience and protect against unprecedented cybercriminal activities.

References

[1] Jewkes, Y., & Yar, M. (2013). Introduction: The Internet, cybercrime and the challenges of the twenty-first century. In Handbook of internet crime (pp. 1-8). Willan.

[2] Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154-176.

[3] Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), 4-37.

[4] Mughal, A. A. (2021). Cybersecurity Architecture for the Cloud: Protecting Network in a Virtual Environment. International Journal of Intelligent Automation and Computing, 4(1), 35-48.

[5] Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the internet of things. In 2015 ieee world congress on services (pp. 21-28). IEEE.

[6] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information fusion, 58, 82-115.

DOI: 10.54254/2755-2721/73/20240409

[7] Jarrett, A., & Choo, K. K. R. (2021). The impact of automation and artificial intelligence on digital forensics. Wiley Interdisciplinary Reviews: Forensic Science, 3(6), e1418.

[8] Jiang, J., Chen, J., Gu, T., Choo, K. K. R., Liu, C., Yu, M., ... & Mohapatra, P. (2019, November). Anomaly detection with graph convolutional networks for insider threat and fraud detection. In MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM) (pp. 109-114). IEEE.

[9] Khaliq, S., Tariq, Z. U. A., & Masood, A. (2020, October). Role of user and entity behavior analytics in detecting insider attacks. In 2020 International Conference on Cyber Warfare and Security (ICCWS) (pp. 1-6). IEEE.

[10] Khan, M. Z. A., Khan, M. M., & Arshad, J. (2022, December). Anomaly Detection and Enterprise Security using User and Entity Behavior Analytics (UEBA). In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) (pp. 1-9). IEEE.

[11] Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences, 11(8), 3383.

[12] Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security, 105, 102258.

[13] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2, 1-18.

[14] Patel, A., Taghavi, M., Bakhtiyari, K., & Júnior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. Journal of network and computer applications, 36(1), 25-41.

[15] Hassan, W. U., Bates, A., & Marino, D. (2020, May). Tactical provenance analysis for endpoint detection and response systems. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 1172-1189). IEEE.