IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 1, Ser. 2 (Jan. – Feb. 2025), PP 69-72
www.iosrjournals.org

Role of AI in Enhancing Cybersecurity: Opportunities and Challenges

Sairup Samal

Abstract:
The paper critically scrutinizes the unhealthy evolution of cyber threats and ethical and executional challenges by the incorporation of Artificial Intelligence in Cybersecurity. It also highlights about the dual use of AI to combat the cyber challenges. The paper also reviews about threat detection, malware classification and network intrusion. The current executional landscape is determined highlighting about the risk based approaches and tension in fostering development and eliminate risks. Ethical concerns such as transparency, accountability and responsibility are explained in depth in the pursuit of the ongoing cyberthreats in different sectors. The paper Is concluded with the pathways for the incorporation of more advanced AI systems and cooperation of the scientists, researchers and industrial leaders to deploy the AI systems to strengthen cybersecurity.

I. Introduction

The contribution of Artificial Intelligence is immense to analyse and eliminate threat detection thereby emerging as an unparalleled innovation to bolster cybersecurity. According to Gartner, the researchers claim in the banking sector around 50 percent have already incorporated AI in the system with a scope to deploy the generative AI which accounts for less than 40 percent. Organisations plan to increase their investments significantly incorporating cybersecurity(89%),generative AI(90%) and broader AI applications(89%).By the implementation of AI and ML, cybersecurity systems detect and analyse the coveted patterns of the data and track the anomalies(if present)by the virtue of more pragmatic decisions to operate, manage namaste preventing the cyberthreats. The paper begins by highlighting the limitations and challenges which arrives with the applications of Machine learning and the vulnerability of Generative AI to adversarial attacks. The paper finally provides the proper research direction and research direction in AI for strengthening cybersecurity through the use of its application such as supervised and unsupervised learning and integration of AI with different security tools and media.

II. Machine Learning Algorithm in Cybersecurity

To brief about the overview of the AI and ML,it can be broadly classified into:

Supervised Learning- Supervised Learning is a model which works based on the principles of input objects and output values enabling the prediction of new, unseen data.It includes malware classification, spam detection.

Unsupervised Learning- Unsupervised Learning is a framework which initiates the grouping of data by detecting patterns and similarities of the clusters of ungrouped data.

Reinforcement Learning- Reinforcement Learning is based on the unfolding of multi faceted problems by the agents through trial and error thereby enhancing the cumulative rewards.

Common Machine Learning Algorithms:

1. **Naive Bayes**- It works on the principle of Bayes Theorem and determines the independence of the conditional features independent of the label class.

2. **Linear Progression**- It is based on the algorithm of supervised learning which acknowledges the labeled data from the given data set and maps the data points to provide the predictions of other datasets.

3. **Logistic Regression-** It is a statistical model based on the supervised learning algorithm which is used to predict binary outcome from a set of independent variables.

4. **Boosting Algorithm-** Boosting algorithm works on the process to generate multiple weak learners and combine their predictions to produce a single rule.

Feature engineering involves selection and transformation of raw data sets to produce more relevant information which is used during the process of Machine learning algorithm.

It is subclassified into feature selection which provides the most relevant and differentiable features to boost model performance and interpretability. Common feature selection methods include embedded methods,filter methods, wrapper methods.

The model being once selected is directed to train using various Algorithms and hyper parameter settings to minimise the predefined loss function.
Appropriate evaluation metrics are used to assess the performance of trained model. It includes accuracy, precision, recalling, ROC curve etc.

Generalization fitting of the model can be determined by proper validation techniques such as k fold cross validation to highlight its efficiency to model a new data and provide a real world estimate of it.

III. Real World Applications:

Case study - Feedzai

One vendor selling anomaly detection-based fraud detection software to banks is Feedzai. The company claims their software can help banks prevent fraud and money laundering by developing detailed risk profiles on customers and scoring them based on granular data.Feedzai claimed to have helped top US retail banks.the client bank found that their current fraud detection process for the online application of their main application processing system had been rejecting over half of the applicants. This resulted in significant losses the bank wanted to prevent in the future.

They needed a risk scoring application that could run through new account applications and only accept those that revealed a low risk rate for fraud. Therefore the client bank incorporated Feedzai's fraud detection software in their main database which provided it the right to execute as principal decision making engine of the arriving customers. The software was also modified to express the follow up questions before making a decision.As a result the client bank saw a rise of 70 percent increase in regular customers and the massive surgery of fraud loss.

Predictive Analysis Fraud Detection-

Crowdfunding website Patreon uses Stripe to process their payments, which a bank using predictive analytics software could recognize as a separate entity. This allows the software to identify the transactions using a third party service to decrease the false positives.

The above case study provides an overview of the machine learning fraud detection in banking systems.
Since the early 2010s, major banks have used anomaly detection – an AI technique for identifying deviations from a norm – for automating fraud, cybersecurity, and anti-money laundering processes.The traditional fraud detection softwares lacked the proficiency to adapt to developed financial fraud risks.

Therefore AI powered fraud detection softwares were installed and has been successful in crypto tracing, verification chat box, E-Commerce fraud detection and is expected to scrutinise several upcoming digital frauds based on the given lines.

Opportunities by AI Enhanced threat detection automated response and predictive analysis:

Incorporation of AI and Cybersecurity deploy AI Enhanced threat detection which achieve detection rates between 80%and 92%.

AI powered user and entity powered behavioural analytics can ameliorate baselines for normal activity and flag detection improving it by 45%.

The automated systems stimulate scalability, workload optimization and minimize human errors.

Predictive analysis utilises traditional data and Algorithms to anticipate human threats and accordingly develops strategies to strengthen the defense system.
Threat Intelligence detection and reduction in false positives improve the efficiency of security operations.

However the existing algorithm is alone insufficient to eliminate a more vulnerable threats and therefore it is needed to be modified:

Hybrid and explainable AI can incorporate supervised, Unsupervised and Reinforcement learning with explainable AI(XAI).Integration with blockchain and quantum resistant security.

AI driven Cybersecurity addresses data privacy and surveillance, accountability, transparency and explainability, job displacement and economic impact.

IV. Challenges And Ethical Concerns

The primary challenge includes the availability of a large volume of sensitive data more accessible which increases the risk of unauthorised data exposure or misuse.

Ensuring compliance with data protection and regulation especially dealing with multi jurisdictions data is complex.

AI models targeted by adverbial attacks such as data poisoning and evasion attacks which can deteriorate evasion accuracy.

Future outlook:The evolving role of AI in cybersecurity and anticipated development-

The rapid proliferation of modern cyberthreats with digital pace of businesses and technology outwit the traditional security algorithms making it complex to extrapolate and mitigate.
Therefore the solution proposed must be of the manufacturing and tertiary sectors must be powered by AI driven cybersecurity in large volume.
By 2030,AI is expected to reach 94 billion dollars in the market of cybersecurity. Further the evolution of AI may enables it to protect the unstructured data and comply with the evolving regulations.

AI driven automation will be sophisticated supporting zero trust architecture and verification. Augmented human analyst powered by AI copilot will significantly ameliorate the decision making capability and are expected to reduce the reaction time.

V. Conclusion:

The rapid evolution of cyber threats and the increasing complexity of modern networks and systems have made traditional cyber security approaches insufficient for effective protection. AI and ML techniques offer powerful tools to enhance cyber security by enabling more proactive, adaptive, and autonomous threat detection and response. This paper has provided a comprehensive overview of the current state and future potential of AI and ML in cyber security. We have discussed the key challenges and limitations of traditional security approaches, and introduced the main categories of ML techniques and their applications in various cyber security domains, including malware detection, network intrusion detection, fraud detection, and user behavior analytics. Real-world case studies have demonstrated the successful implementation of AI and ML in cyber security, highlighting their ability to detect novel and evolving threats that may evade traditional security measures. However, we have also discussed the challenges and limitations of applying AI and ML in cyber security, such as data quality issues, adversarial attacks, interpretability concerns, and scalability challenges. Looking forward, we have identified several promising research directions and opportunities for advancing the field of AI-powered cyber security. These include the development of explainable AI techniques, adversarial machine learning, transfer learning, autonomous and adaptive security, collaborative and federated learning, and integration with security orchestration and automation platforms. By embracing these technologies and investing in their development and deployment, we can build a more resilient, safe and secure future.

Bibliography

[1]. J. Hong, "The state of phishing attacks," Communications of the ACM, vol. 55, no. 1, pp. 74-81, 2012. [10]
[2]. P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in IFIP International Conference on Communications and Multimedia Security, 2014, pp. 63-72: Springer. [11]
[3]. C. Colwill, "Human factors in information security: The insider threat–Who can you trust these days?," Information security technical report, vol. 14, no. 4, pp. 186-196, 2009. [12]
[4]. S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE communications surveys & tutorials, vol. 15, no. 4, pp. 2046-2069, 2013. [13]
[5]. D. E. Denning, "An intrusion-detection model," IEEE Transactions on software engineering, no. 2, pp. 222-232, 1987. [14]
[6]. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection:

Techniques, systems and challenges," computers & security, vol. 28, no. 1-2, pp. 18-28, 2009. [15]
[7]. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," Ieee communications surveys & tutorials, vol. 16, no. 1, pp. 303-336, 2013. [16]
[8]. C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," Journal of network and computer applications, vol. 36, no. 1, pp. 42-57, 2013. [17]
[9]. N. Miloslavskaya and A. Tolstoy, "Application of big data, fast data, and data lake concepts to information security issues," in 2016 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2016, pp. 148-153: IEEE. [18]
[10]. Y. Xin et al., "Machine learning and deep learning methods for cyber security," Ieee access, vol. 6, pp. 35365-35381, 2018. [19]
[11]. M. Alazab, S. Venkatraman, P. Watters, M. Alazab, and A. Alazab, "Cybercrime: The case of obfuscated malware," in Global Security, Safety and Sustainability & e-Democracy: Springer, 2012, pp. 204-211. [20]
[12]. E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," ACM Computing Surveys (CSUR), vol. 47, no. 4, pp. 1-33, 2015. [21]
[13]. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications surveys & tutorials, vol. 18, no. 2, pp. 1153-1176, 2015. [22]
[14]. Amit, J. Matherly, W. Hewlett, Z. Xu, Y. Meshi, and Y. Weinberger, "Machine learning in cyber-security-problems, challenges and data sets," arXiv preprint arXiv:1812.07858, 2018. [23]
[15]. E. Alpaydin, Introduction to machine learning. MIT Press, 2020. [24]
[16]. S. B. Kotsiantis, I. Zaharakis, and P. Pintelas, "Supervised machine learning6282 Dr. Nirvikar Katiyar / Kuey, 30(4), 2377 [60]
[17]. Darktrace, "Darktrace Cyber AI Platform," 2021, https://darktrace.com/en/platform/. [61]
[18]. Tan, "AI-Based Cyber Defense: The Future of Cyber security?," 2019, https://www.darktrace.com/en/blog/ai-based-cyber-defense-the-future-of-cyber security/. [62]
[19]. Darktrace, "Use Case: Insider Threat," 2021, https://darktrace.com/en/resources/wp-insider-threat.pdf. [63]
[20]. Darktrace, "Case Study: Major US Retailer," 2021, https://darktrace.com/en/resources/cs-major-us-retailer.pdf. [64]
[21]. Darktrace, "Case Study: European Bank," 2021, https://darktrace.com/en/resources/cs-european-bank.pdf. [65]