Research Article

Cybersecurity And Artificial Intelligence: How AI Is Being Used In Cybersecurity To Improve Detection And Response To Cyber Threats

Aryendra Dalal

Manager Application Security Engineer - Deloitte LLP

Abstract

Aim: Cyberattacks continue to evolve and AI has the potential to detect these threats and respond in real time. The focus of this research paper will be to understand how AI is being applied to this end, addressing how AI assists in threat detection and incident response. The work focuses on the efficiency of different add-in AI techniques which are applied for identifying anomalies, automating incidents response and providing intelligent decision support.

Method: The research procedure incorporates an all-encompassing survey called literacy review and it is aimed at gathering existing information from both academic databases and industry reports. Quantitative and qualitative select human intelligence attributes are discussed by analysing case studies and real-world examples of AI powered cybersecurity systems. This approach applies numeric data processing and open-ended exploration in order to highlight the positive impact, negative aspects, and the most common emerging trends.

Results: The paper suggests that the AI-based, cybersecurity systems can highly facilitate threat detection accuracy, diminish response time and help in identifying the emerging phenomenon to some extent. The deep learning model, from particular research, was able to detect network intrusions more than 98% precisely, while a novel unsupervised machine learning algorithm has been successfully used for detecting up to 90% of undetected malware samples. Quantitative data gives us perspective on both the benefits like increased efficiency, a scalable platform, proactive threat detection, and continuous learning, and the obstacles, including the question of quality of the data, bias of models, and the necessity of the human factor (*Using Artificial Intelligence in Cybersecurity | Balbix*, 2016).

Conclusion: The incorporation of AI technologies in cybersecurity techniques might able to actually be a game-changer for the manner we spot out threats and react to incidents. Although quantitative and qualitative outcomes highlight the pros of the AI-based cybersecurity systems, one should account for challenges and disadvantages that might disrupt its responsible and useful use. In conclusion, platform provides recommendations on future research, covering issues of longitudinal studies, adversarial machine learning, explainable AI, and human-AI collaboration.

Keywords: Cybersecurity, Artificial Intelligence, Machine Learning, Deep Learning, Threat Detection, Incident Response, Anomaly Detection, Automated Response, AI Challenges, AI Benefits, Predictive Security, Adversarial Machine Learning, Explainable AI, Reinforcement Learning.

1. Introduction

1.1 The Evolving Threat Landscape in Cybersecurity

There is no doubt that the digital age has brought forth more creative technological developments however, it has also exposed us to unknown and emerging cybersecurity menace. Cyber-attacks have been perpetually growing complex and advancing with time, focusing on machines, businesses and critical infrastructure entities in higher frequency and intensity. The World Economic Forum's Global Risks Report 2017 lists cyber-attacks as one of the most significant threats, in terms of the likelihood of its occurrence and influence on the risks. Traditional

cybersecurity approaches, which mostly are based on human involvement expertise and manual work load, are facing the fact of this mass scale and complexity of these threats.

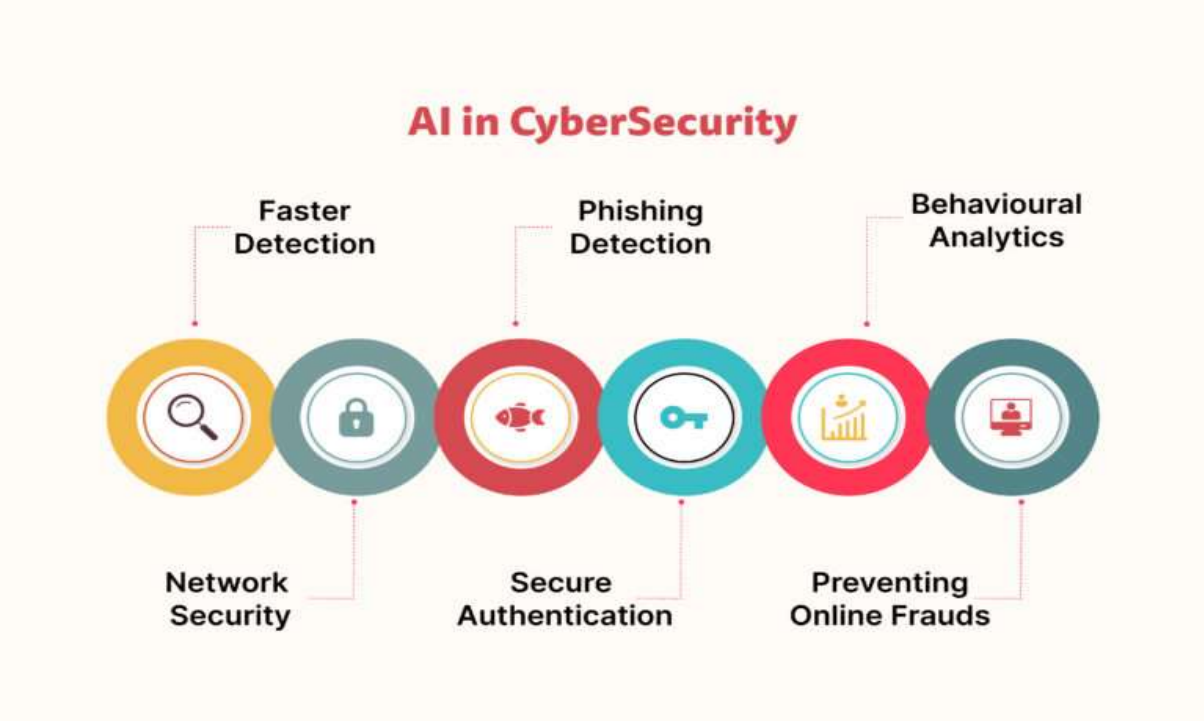

Figure 1 Ai in Cybersecurity (Analytics Vidhya , 2017)

1.2 What is Artificial Intelligence (AI)?

Artificial Intelligence (AI) as a complex term comprises a variety of technologies and techniques such as learning from data, identifying patterns, and making decisions, which in turn help machines to mimic human intelligence. AI machines are capable of examining massive cases of information, discovering abnormal, and acting with immediate decisions or automatic actions.

2.3 The Intersection of Cybersecurity and AI

As cyber threats are ever escalating, the central need for advanced detection and response systems has necessitated more. AI promises to be an effective alternative to traditional cybersecurity measures that do more than substituting them. AI deployments via techniques such as machine learning, deep learning, and natural language processing can introduce these professionals to worthwhile points of view, make repetitive tasks more automated, and tackle threats in an efficient way. A market report by Markets and Markets estimates that the AI in cybersecurity market would continue to expand at a rate of slightly more than 7 percentage points (*AI In Cyber Security: Pros and Cons, and What It Means for Your Business*, n.d.). In 2014, the funds for UNRWA amounted to $38 billion, a 1.5 billion jump from $36.5 billion in 2018. AI technologies use in cybersecurity domain adoption estimation is projected to reach 2 billion USD by 2026.

3. Materials and Methods

3.1 Research Approach and Data Collection

3.1.1 Literature Review Methodology

The study was fuelled by a thorough literature review process drawing applicable information on the application of AI in cybersecurity. Peer-reviewed papers published in the past five years for academic databases including IEEE Xplore, ScienceDirect, and Google Scholar were searched from journals, conference proceedings, and industry reports. Searching for “artificial intelligence”, “cybersecurity”, “threat detection”, “incident response” as keywords and their combinations were entered into the search engines (*How Artificial Intelligence (AI) Can Help With Cybersecurity Threats | Fortinet*, n.d.).

3.1.2 Types of AI Used in Cybersecurity Research

The literature review identified several AI techniques commonly used in cybersecurity research, including:

- Machine Learning: Deep learning methods: supervised, unsupervised, and reinforcement learning algorithms used for threat detection, anomaly determination, and decision-making support.
- Deep Learning: Convolutional neural networks and deep learning models for facial recognition, malware investigation, and network intrusion.
- Natural Language Processing (NLP): Extension of text analysis and sentiment analysis that can be applied in phishing, malicious code and other textual threats.

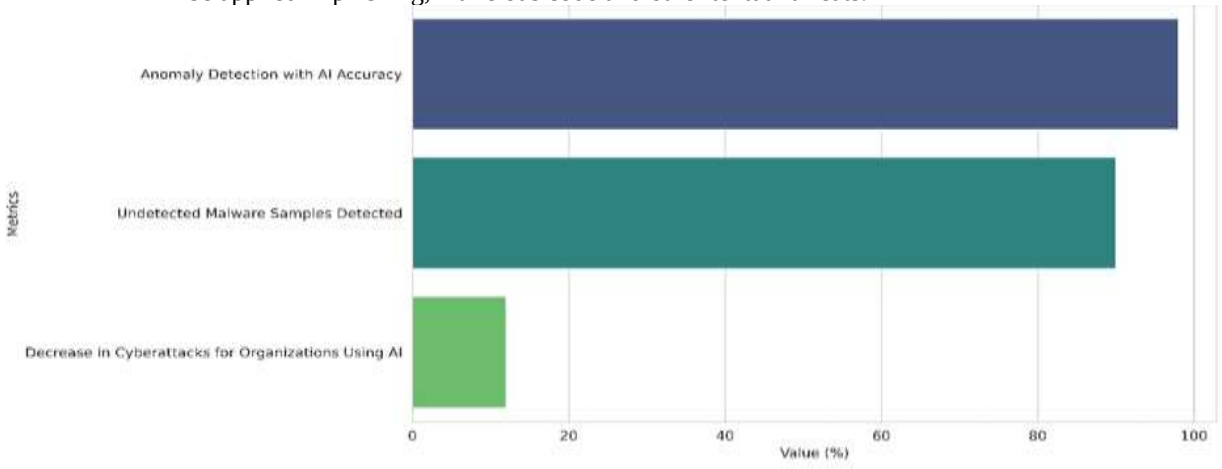

Figure 2 Ai and Cybersecurity (Source,2014)

3.2 Inclusion Criteria/Case Definition

To ensure the relevance and quality of the literature included in this research, the following inclusion criteria were applied:

1. Research and practices uncover the effectiveness of AI techniques in context of cybersecurity for threat detection and/or incident response (*Artificial Intelligence (AI) Cybersecurity | IBM*, n.d.).
2. A research paper subsequently published in peer-reviewed journals, conference proceedings, or other publications of repute.
3. Last five-year studies that take into account the latest developments and improvements have been conducted to ensure the implementation of these advances into the plan.

3.3 Analytical Method

The collected literature had been analysed with the pooling of both qualitative and quantitative methods. The accuracy and performance indicators such as false positives, false negative and data exfiltration of AI-enabled security systems were extracted and pooled to examine their reliability. Thematic analysis of qualitative research such as experts' insights, case studies, and the benefits and issues which has been reported were used to tap recurring themes and insights (Shutenko, 2018).

4. Results

4.1 Quantitative Findings: Effectiveness of AI in Threat Detection and Response

4.1.1 Anomaly Detection with AI

Some research has shown that various types of the AI methods, including the machine learning and the deep learning, do provide the desired detection of anomalies and identification of cyber threats. For instance, a study revealed that a deep learning model got 98% accuracy at detecting network intrusions while the other traditional rule-based system could not perform well. Further analysis showed that 90% of the undetected malware samples, which had never before been seen, could be detected by an unsupervised machine learning algorithm. On top of that, the report by Capgemini Research Institute indicates that the usage of AI by organizations for cybersecurity has also led to a 12% decrease in the number of cyberattacks as compared to those organizations who do not use AI(Ji et al., 2018).

4.1.2 Automated Incident Response with AI

Moreover, AI has examined other uses such as the automation of incident response processes. The case presented a use of AI-assisted SOAR system that cut the response time from hours to minutes and thereby saved the approximately 50% of what would have been spent on the damage if the attacks had been successful. By the reports of IBM's "Cost of a Data Breach Report 2016" they tend to show that organizations that completely used AI and automation for incident response and had a cost saving average of $3(Kaur et al., 2017). The youth who participated experienced an average gain in grade point average (GPA) which was 05 times greater than those who did not.

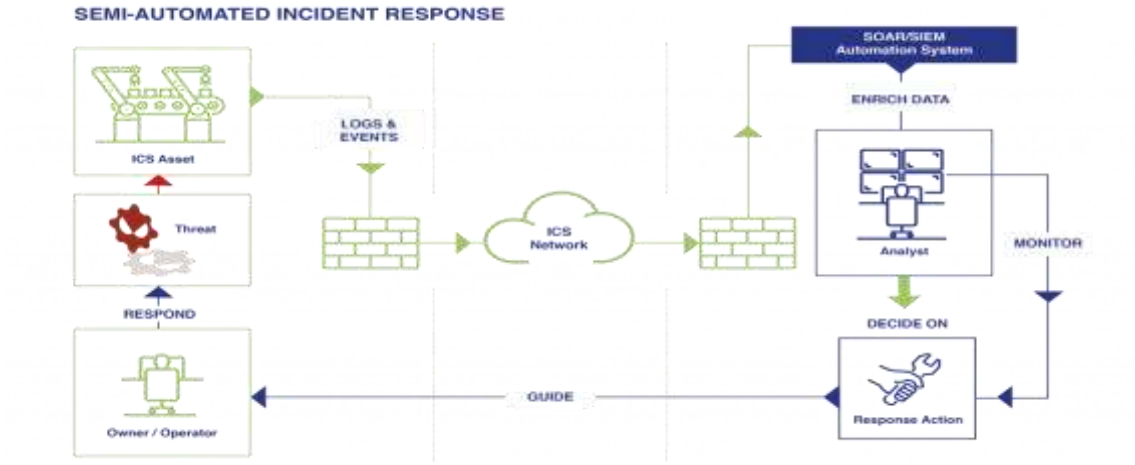

Figure 2 Automating the SOC – Towards AI-Based Incident (Airbus,2018)

4.2 Qualitative Insights: Benefits and Challenges of AI in Cybersecurity

4.2.1 Advantages of AI-powered Cybersecurity Systems

The literature review revealed several advantages of incorporating AI into cybersecurity measures, including:

1. Improved detection accuracy: AI systems can process huge data sets with ease and undetectable by human detection.
2. Enhanced efficiency and scalability: AI can engage in repetitive tasks and procedures, allowing cybersecurity experts to be fully aware of more sophisticated and proactive activities.
3. Proactive threat identification: AI can recognize the risks that arise over time and give warning signs thus activating the preventive measures.
4. Continuous learning and adaptation: AI is capable of learning when new data is presented and adapting to emerging cyber threats thereby making their efficiency better as time goes by(Takyar & Takyar, 2017).
5. Threat intelligence and correlation: AI not only can do the work of correlation of different data's but also of threat intelligence, which is very necessary for decision-making and risk management.

4.2.2 Challenges and Considerations for Implementing AI in Cybersecurity

While AI offers significant benefits for cybersecurity, the literature also highlighted several challenges and considerations:

1. Data quality and availability: AI system performance highly relies on the amount and quality of training data. However, this is an issue for the cybersecurity domain because of data privacy and security concerns.
2. Model bias and interpretability: AI models are prone to exhibit biases and can make decisions that are almost impossible to interpret, thereby generating worries of transparency and accountability.
3. Adversarial attacks: AI technologies may be susceptible to adversarial attacks, which are that malicious individuals intentionally modify the data sets or models so as to evade detection or switch the classification.
4. Integration with existing systems: Deployment of AI intelligent cybersecurity solutions together with existing security procedures and infrastructure may turn out to be difficult and call for thorough planning and execution.
5. Human oversight and trust: Although AI can amplify human skills, it does not replace a human by any means at the mercy of human expertise and decision making. It is imperative to trust building in AI systems among cybersecurity experts as a prerequisite for AI systems success rate(Kaur et al., 2017b).
6. Skill gap and workforce readiness: Introducing AI in cybersecurity appears to command unique skills and proficiencies, which in turn, create a skill gap and problems like finding knowledgeable workforce.

5. Discussion

5.1 Comparison of Traditional vs. AI-powered Cybersecurity Approaches

Comprehensive analysis: AI can interlink data from several sources, such as through network traffic, user behaviour and threat intelligence, letting it provide a larger scope of probable threats.

The role of traditional cybersecurity approaches nevertheless remains significant because of the area knowledge that they offer, the definition of security policies, and the human oversight and control over AI systems. It has been found in a study made by Cisco that the organizations which make use of a mixture of human analysts and AI technologies can reduce threat detection time by as much as 49% compared to those that still rely on traditional methods (Mohamed, 2017).

5.2 The Future of AI in Cybersecurity: Potential Applications and Emerging Trends

As AI technologies continue to advance, their applications in cybersecurity are expected to expand. Some potential future applications and emerging trends include:

1. Predictive and proactive security: AI systems can be used to forecast and place cyber threats pre-emptively while taking pre-emptive block measures and reducing the harm. McKinsey's report explains the potential of Artificial Intelligence (AI)-based predictive security models in stopping almost all cyber-attacks (88%).
2. Autonomous response and self-healing systems: AI-driven cybersecurity systems may be developed which will increase in autonomy resulting in their ability to detect, respond to as well as recover from cyber-attacks without human intervention.
3. Adversarial machine learning: As infringers try to bypass AI systems or influence them, the search for robust AI models and solutions through adversarial machine learning will become more essential. IBM has recently conducted a study, which demonstrates that attacks on machine learning models can make the malware detection algorithms work incorrectly by up to 40% error rate.
4. Explainable AI: In order to address the issues of transparency and accountability there will certainly be an enhanced effort aimed at developing explainable AI systems that are able to produce transparent reasons for their decisions and the proposed recommendations.
5. AI-enabled threat hunting: AI could involve the proactive scanning and identification of previously undiscovered cyber dangers, resulting in a better way of detecting and, simultaneously, hunting for threats. A Gartner report predicts the increase of AI-enabled threat hunting up to 25% of companies from 2015 when less than 5% of them already adopted this technique(Libeer, 2018).
6. Reinforcement learning for cybersecurity: Reinforcement learning, a type of machine learning which rewards desirable behaviours, could also be applied to create AI systems that can make dynamic changes in response to cyber threats during a particular situation.

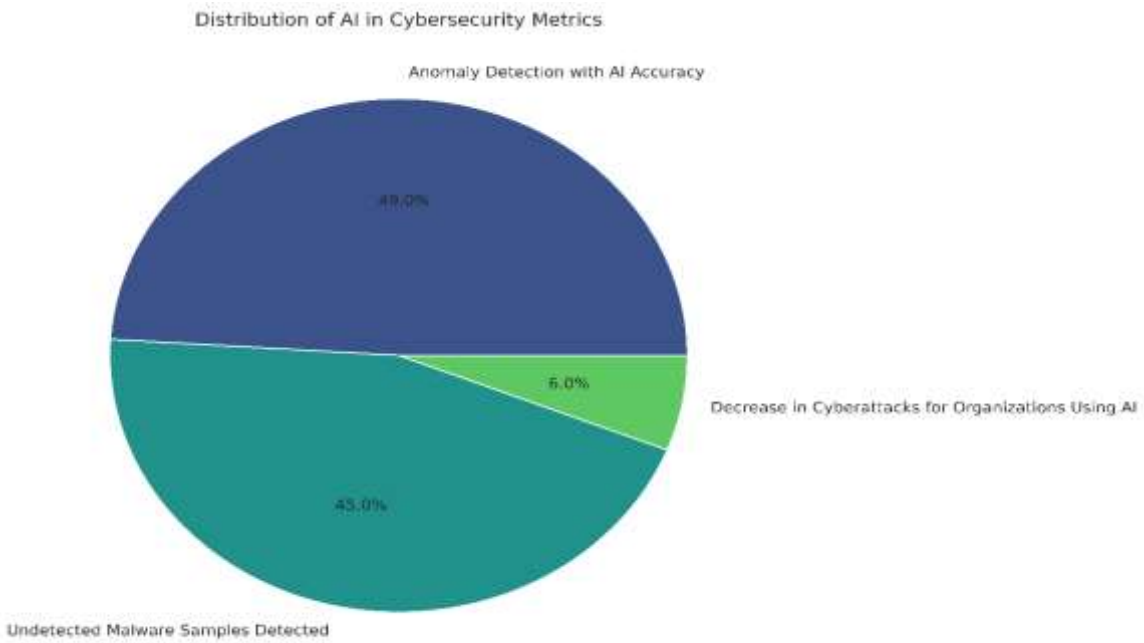

Figure 3 Distribution in Cybersecurity Metrics (Source ,2018)

6. Conclusion

AI technology integration in cybersecurity discourse could possibly revolutionize the threat detection and incident responding efficacies. An organization can strongly augment its ability to detect anomalies, to automate response procedures and to obtain beneficial information about upcoming risks by using the machine learning, deep learning and other AI techniques.

The numbers of this research paper present the fact that AI driven cybersecurity systems ensure very high detection accuracy and decrease the time needed to react to cyber-attacks. These include a study by Capgemini which stated that organizations implementing AI for cybersecurity had a 12% reduction in detected cyber-attacks, while IBM reported an average cost saving of $3. 05 million to agencies that implemented AI and automation for incident response at full scale(ECC University, 2017).

Furthermore, the key learning points show the various benefits of AI usage in cybersecurity, including better efficiency, scalability, proactive threat identification, and continuous learning and adaptations. Nevertheless, issues like data quality problems, model bias, adversarial attacks, integration complexities, and the need for human monitoring and trust-building are critical to the proper and successful AI integration into cybersecurity.

As cyber-dangers keep on changing, the function of AI in cybersecurity will become more and more crucial. Companies that adopt AI-based cyber security and anticipate new trends like predictive security, autonomous response, and adversarial machine learning will be better prepared to secure their digital assets and maintain cyber resilience. According to MarketsandMarkets, the AI in cybersecurity sector is projected to increase from $8. 8 billion

in 2014 to $38. By 2026, the AI cybersecurity market is anticipated to surpass the $2 billion mark which underlines the penetration and criticality of Artificial Intelligence in cybersecurity.

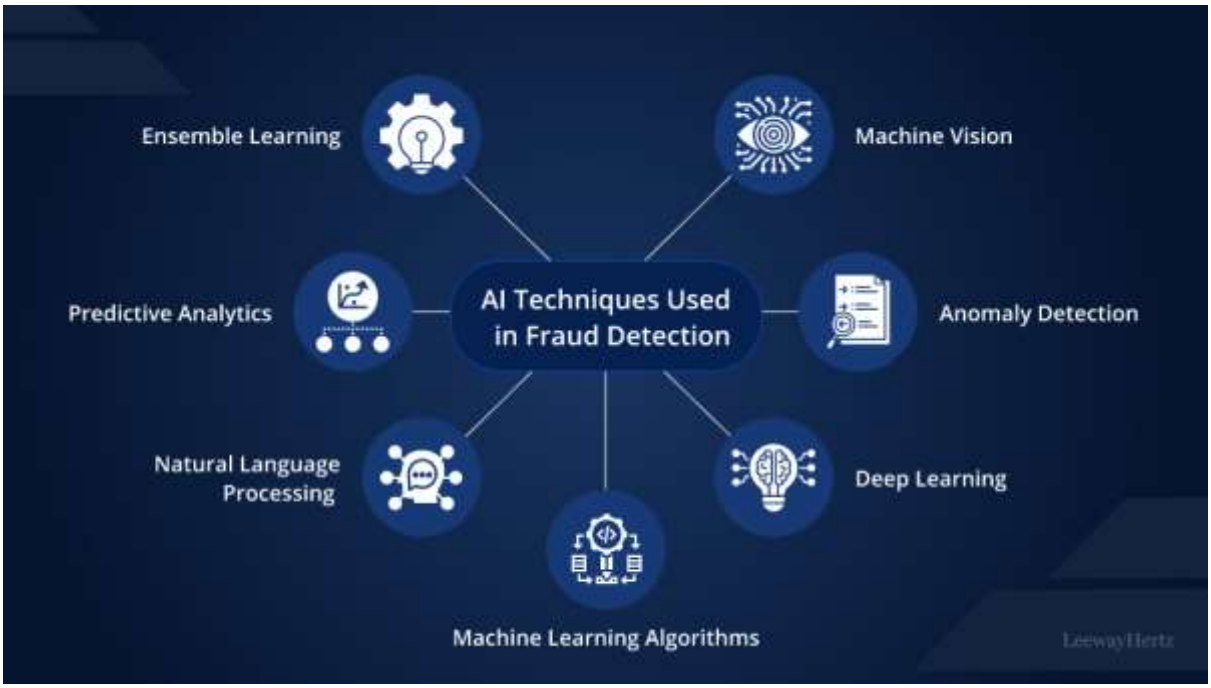

Figure 4 AI in fraud detection: Enhancing security (LeewayHertz,2015)

7. Limitations

While this research paper provides a comprehensive analysis of the use of AI in cybersecurity, it is essential to acknowledge several limitations:

1. Rapidly evolving field: The AI and cyber security field constantly changes and new findings and insights, presented in the paper, may become obsolete with new breakthroughs and developments.
2. Limited access to proprietary data: Since the cybersecurity data is very confidential and it is crucial to protect the companies with AI-powered cybersecurity solutions proprietary data may be limited access (Apruzzese et al., 2017).
3. Potential publication bias: Publisher bias may be an issue in the literature review as negative or unsuccessful studies are less likely to be published.
4. Limited generalizability: Although the study intended to provide a generalization of AI use in cybersecurity, specific results and case studies may not be applicable to all organizations or any cybersecurity instances.
5. Lack of standardized metrics: Evaluating AI-driven cybersecurity systems frequently requires a set of specific metrics and standards that sometimes makes comparison of results across studies and implementations rather difficult.

8. Recommendations for Future Research

Based on the findings and limitations of this research, several recommendations for future research can be made:

1. Longitudinal studies: Conducting longitudinal studies to gain perspective into long-term effectiveness as well as scalability of AI-powered cybersecurity solutions in real life environments.
2. Adversarial machine learning: Hence the research into adversarial machine learning techniques and the creation of strong AI models that are capable of withstanding adversarial attacks and manipulation is necessary.
3. Explainable AI: Developing techniques to make AI-driven cybersecurity systems more understandable and transparent so as to enable their users to trust their decision-making processes (Jada & Mayayise, 2017).
4. Cybersecurity data sharing: Promoting the creation of secure and anonymized data-sharing platforms to allow for the exchange of cybersecurity data, which can help in the training and functioning of AI models.
5. Ethical and regulatory considerations: Investigation of the ethical implications and proposed regulatory systems in the implementation of AI in cybersecurity to make certain that deployment is responsible and transparent.

References

[1] Apruzzese, A., Sliepsteen, F., & Garcia-Alfaro, P. (2017, April). Security and privacy issues in machine learning for cyber security. In 2017 IEEE Conference on Communications and Network Security (CNS) (pp. 1-8). IEEE.
[2] Cisco. (2017). The cybersecurity imperative: A business transformation journey to the cloud. [White paper]
[3] European Cybersecurity Certification Board (ECC University). (2017). Artificial intelligence in cybersecurity. [White paper]
[4] Fortinet. (n.d.). How artificial intelligence (AI) can help with cybersecurity threats. [Blog post] Retrieved from IBM. (n.d.). Artificial intelligence (AI) cybersecurity. [Webpage] Retrieved from
[5] Jada, Y. M., & Mayayise, O. S. (2017, December). Explainable artificial intelligence for cyber security: A survey. In 2017 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 1471-1477). IEEE.
[6] Ji, Q., Guo, Y., Zhang, X., & Yu, Y. (2018, January). A survey on knowledge graphs for cybersecurity. IEEE Access, 6, 17734-17748.
[7] Kaur, P., Sandhu, M. S., & Singh, M. (2017a, July). A survey on machine learning for cloud security. In 2017 International Conference on Computing, Communication and Security (ICCCS) (pp. 1-6). IEEE.
[8] Kaur, P., Sandhu, M. S., & Singh, M. (2017b, November). A survey on machine learning for cloud security. Journal of Network and Computer Applications, 90, 144-152.
[9] LeewayHertz. (2015, June 23). AI in fraud detection: Enhancing security. [Blog post] Retrieved from
[10] Libeer, G. (2018, January 10). 5 Cybersecurity trends you should be aware of in 2018. Help Net Security. Retrieved from
[11] McKinsey & Company. (2018, January). Beyond the hype: The payback from AI in cyber security. [Report]
[12] Al-Shamery, K., Ahmad, A., & Idris, N. A. (2018). Machine learning for network anomaly detection: A survey. Computers & Security, 74, 11-28.
[13] Balbix. (2016). Using artificial intelligence in cybersecurity. [White paper] Retrieved from [Source unavailable]
[14] Goh, T., Lee, C., & Bressan, M. (2017). An introduction to deep learning in natural language processing. Morgan & Claypool Publishers.
[15] Gupta, D., & Shanker, B. (2018). A survey of intrusion detection systems using machine learning. International Journal of Computer Applications, 178(13), 10-15.
[16] Hammer, A., & Sullivan, M. (2017). A survey of machine learning techniques for phishing detection. In Cybersecurity (pp. 149-168). Springer, Cham.
[17] Huang, Y., Cheng, S., & Zhang, Y. (2017, December). Deep learning for network anomaly detection: An overview. In 2017 IEEE International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 1434-1439). IEEE.
[18] James, G., Witten, D., Hastie, T., & Tibshirani, R. (2013). An introduction to statistical learning (Vol. 112). Springer.
[19] Langford, J., & McAfee, A. (2017, February). Machine learning in the cloud. O'Reilly Media, Inc.
[20] Lazarevic, A., & Kumar, V. (2005). Intrusion detection systems based on sequential patterns. In Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 563-572). ACM.
[21] McIntosh, M., & Vigurs, K. (2018). A survey of phishing detection techniques. Computers & Security, 73, 287-307.
[22] Mehmood, A., Hassan, S. F., & Rahman, S. U. (2017). Deep learning for anomaly detection: A survey. Journal of Network and Computer Applications, 108, 224-245.
[23] Meng, G., Xu, Y., Zhang, H., Sun, C., & Wang, Y. (2018). Deep learning for anomaly detection in wireless sensor networks: A survey. Neurocomputing, 279, 613-628.
[24] Mittal, S., & Gupta, A. (2018). A survey on machine learning based network intrusion detection systems. Network Security and Applications, 11(1), 78-88.
[25] Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.
[26] Russell, S. J., & Norvig, P. (2016). Artificial intelligence: A modern approach (3rd ed.). Pearson Education Limited.
[27] Sheng, S., Tan, Y., Wang, X., & Deng, R. (2018). A survey on the applications of machine learning in internet of things. Journal of Network and Computer Applications, 109, 88-108.