Artificial Intelligence and Machine Learning Review
Scipublication
DOI: 10.69987/AIMLR.2021.20301

The Role of Artificial Intelligence in Cybersecurity: A Review of Threat Detection and Mitigation Techniques

Jorge Silva[1], Maria Gomez[2]
Department of Systems Engineering, Universidad de Cuenca[1], Ecuador, School of Computing, Universidad Nacional de Loja, Ecuador[2]
jorge.silva@ucuenca.edu.ec[1], maria.gomez@unl.edu.ec[2]

Keywords

Artificial Intelligence,
Cybersecurity,
Threat Detection,
Mitigation Techniques,
Machine Learning,
Deep Learning,
Natural Language Processing

Abstract

The rapid evolution of cyber threats has necessitated the development of advanced techniques for threat detection and mitigation. As cyberattacks grow in sophistication and frequency, traditional cybersecurity measures are increasingly inadequate. Artificial Intelligence (AI) has emerged as a pivotal tool in enhancing cybersecurity, offering innovative solutions to detect, analyze, and neutralize threats in real-time. This article provides a comprehensive review of the role of AI in cybersecurity, with a specific focus on its application in threat detection and mitigation. It explores various AI techniques, including machine learning (ML), deep learning (DL), and natural language processing (NLP), and evaluates their effectiveness in identifying and countering cyber threats. ML algorithms, for instance, excel in pattern recognition and anomaly detection, while DL models are adept at handling complex, unstructured data. NLP, on the other hand, plays a crucial role in analyzing textual data to identify phishing attempts or malicious communications. Despite its potential, the integration of AI in cybersecurity is not without challenges. Issues such as data privacy, algorithmic bias, and the need for large datasets for training AI models pose significant limitations. Additionally, adversaries are increasingly leveraging AI to develop more advanced attacks, creating an ongoing arms race. The article also proposes future research directions, emphasizing the need for robust, explainable AI systems and collaborative frameworks to address emerging threats. To support the discussion, three related tables are included, summarizing key findings, comparing AI techniques, and presenting case studies of AI-driven cybersecurity solutions. This review underscores the transformative potential of AI in cybersecurity while highlighting the importance of addressing its limitations to ensure a secure digital future.

Introduction

The digital age has brought about unprecedented advancements in technology, but it has also introduced a myriad of cybersecurity challenges. As cyber threats become more sophisticated, traditional security measures are often inadequate in providing robust protection. Artificial Intelligence (AI) has emerged as a transformative force in the field of cybersecurity, offering innovative solutions for threat detection and mitigation[1]. This article aims to provide a detailed review of the role of AI in cybersecurity, with a particular focus on its application in identifying and neutralizing cyber threats.

The increasing complexity of cyber threats, such as ransomware, phishing, and advanced persistent threats (APTs), has necessitated the development of more advanced and adaptive security measures. AI, with its ability to analyze vast amounts of data and identify patterns, has proven to be a valuable asset in the fight against cybercrime. This article will explore various AI techniques, including machine learning, deep learning, and natural language processing, and their effectiveness in enhancing cybersecurity measures[2].

The Evolution of Cyber Threats

The landscape of cyber threats has evolved significantly over the past few decades. In the early days of the internet, cyber threats were relatively simple, often involving basic viruses and malware. However, as technology has advanced, so too have the tactics and techniques employed by cybercriminals. Today, cyber threats are more sophisticated, targeted, and damaging than ever before[3].

One of the most significant developments in the evolution of cyber threats is the rise of Advanced

Persistent Threats (APTs). APTs are prolonged and targeted cyberattacks in which an intruder gains access to a network and remains undetected for an extended period. These attacks are often carried out by well-funded and highly skilled adversaries, such as nation-states or organized crime groups. APTs are particularly challenging to detect and mitigate due to their stealthy nature and the use of advanced techniques, such as zero-day exploits and custom malware[4].

Table 1: Comparison of AI Techniques in Cybersecurity

AI Technique	Description	Applications in Cybersecurity	Strengths	Limitations
Machine Learning	Algorithms trained to recognize patterns in data.	Anomaly detection, malware detection, phishing detection.	- Detects unknown threats. - Scalable for large datasets. - Adapts to new threats.	- Requires high-quality data. - Vulnerable to adversarial attacks. - High false positives.
Deep Learning	Subset of ML using neural networks to process unstructured data.	Malware detection, network traffic analysis, image-based threat detection.	- Automates feature extraction. - Handles large volumes of data. - High accuracy.	- Computationally intensive. - Requires massive datasets. - Lack of interpretability.
Natural Language Processing (NLP)	AI technique for analyzing and understanding human language.	Phishing email detection, sentiment analysis, insider threat detection.	- Understands human language. - Detects social engineering attacks. - Real-time analysis.	- Struggles with context in complex language. - Limited by language diversity.
Reinforcement Learning	AI learns by interacting with an environment and receiving feedback.	Automated incident response, adaptive threat mitigation.	- Adapts to dynamic environments. - Improves over time. - Optimizes decision-making.	- Requires extensive training. - Limited by the quality of feedback.

Another major trend in the evolution of cyber threats is the increasing use of social engineering tactics, such as phishing and spear-phishing. These attacks involve tricking individuals into revealing sensitive information, such as passwords or credit card numbers, by posing as a trustworthy entity. Social engineering attacks are particularly effective because they exploit human psychology rather than technical vulnerabilities[5].

The rise of the Internet of Things (IoT) has also introduced new cybersecurity challenges. IoT devices, such as smart home appliances and wearable technology, are often designed with limited security features, making them vulnerable to cyberattacks. The proliferation of IoT devices has created a vast attack surface, providing cybercriminals with numerous entry points into networks[6].

The Role of AI in Cybersecurity

Artificial Intelligence (AI) has emerged as a powerful tool in the fight against cyber threats. AI refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. In the context of cybersecurity, AI can be used to analyze vast

amounts of data, identify patterns, and detect anomalies that may indicate a cyber threat[7].

One of the key advantages of AI in cybersecurity is its ability to process and analyze large volumes of data in real-time. Traditional security measures often rely on rule-based systems, which can be limited in their ability to detect new and emerging threats. AI, on the other hand, can continuously learn and adapt to new threats, making it a more effective tool for threat detection.

AI can also be used to automate various aspects of cybersecurity, such as threat detection, incident response, and vulnerability management. Automation can help to reduce the workload on cybersecurity professionals, allowing them to focus on more complex tasks. Additionally, AI-driven automation can help to improve the speed and accuracy of threat detection and response, reducing the time it takes to identify and mitigate cyber threats[8].

AI Techniques in Cybersecurity

There are several AI techniques that are commonly used in cybersecurity, including machine learning, deep learning, and natural language processing. Each of these techniques has its own strengths and limitations, and they can be used in combination to provide a more comprehensive approach to cybersecurity.

Machine Learning

Machine learning is a subset of AI that involves training algorithms to recognize patterns in data. In the context of cybersecurity, machine learning can be used to analyze network traffic, identify anomalies, and detect potential threats. Machine learning algorithms can be trained on large datasets of known threats, allowing them to recognize similar patterns in new data.

One of the key advantages of machine learning is its ability to detect previously unknown threats. Traditional security measures often rely on signature-based detection, which can only identify threats that have been previously encountered. Machine learning, on the other hand, can identify new and emerging threats by analyzing patterns in data[9].

There are several types of machine learning algorithms that are commonly used in cybersecurity, including supervised learning, unsupervised learning, and reinforcement learning. Supervised learning involves training an algorithm on a labeled dataset, where the correct output is known. Unsupervised learning, on the other hand, involves training an algorithm on an unlabeled dataset, where the correct output is not known. Reinforcement learning involves training an algorithm to make decisions based on feedback from its environment[10].

Deep Learning

Deep learning is a subset of machine learning that involves training artificial neural networks to recognize patterns in data. Deep learning algorithms are particularly effective at processing large amounts of unstructured data, such as images, audio, and text. In the context of cybersecurity, deep learning can be used to analyze network traffic, detect malware, and identify phishing emails.

One of the key advantages of deep learning is its ability to automatically extract features from data. Traditional machine learning algorithms often require manual feature extraction, which can be time-consuming and error-prone. Deep learning algorithms, on the other hand, can automatically learn and extract features from data, making them more effective at identifying complex patterns[11].

Deep learning algorithms are also highly scalable, making them suitable for processing large volumes of data. This is particularly important in the context of cybersecurity, where the volume of data generated by network traffic can be overwhelming. Deep learning algorithms can process this data in real-time, allowing for faster and more accurate threat detection.

Natural Language Processing

Natural language processing (NLP) is a subset of AI that involves the interaction between computers and human language. In the context of cybersecurity, NLP can be used to analyze text-based data, such as emails, chat logs, and social media posts, to identify potential threats. NLP algorithms can be used to detect phishing emails, identify malicious content, and analyze the sentiment of text to identify potential insider threats[12].

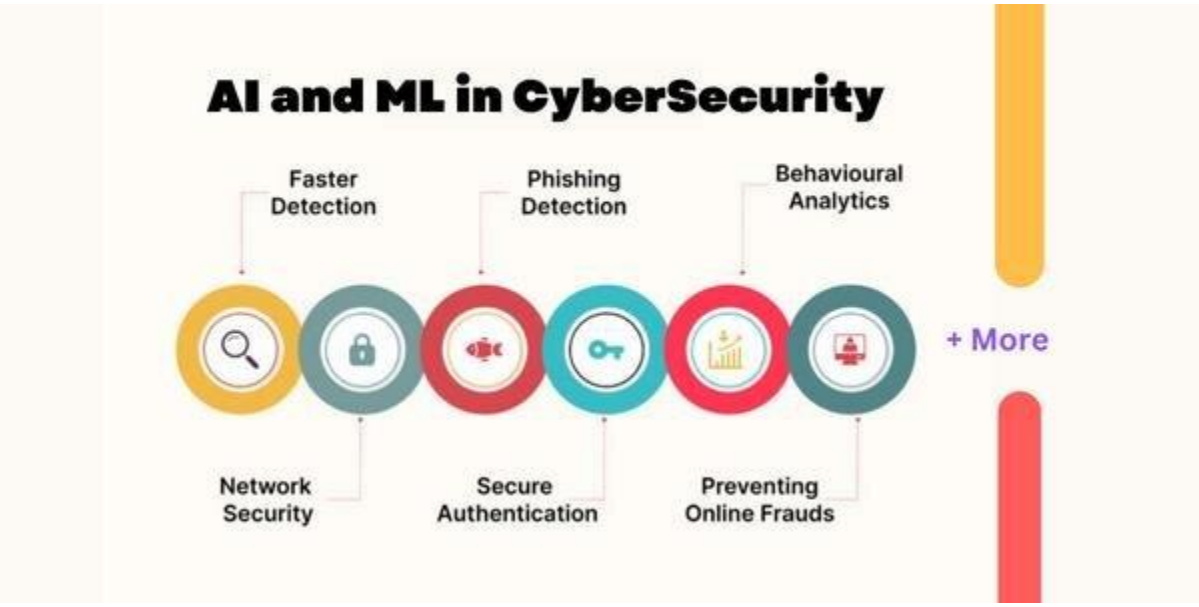
Table 2: Case Studies of AI-Driven Cybersecurity Solutions

Case Study	AI Technique Used	Application	Outcome	Challenges Faced
Darktrace	Machine Learning	Real-time anomaly detection in network traffic.	- Detected insider threats and APTs. - Reduced response time to threats.	- High false positives. - Requires continuous tuning.
Cylance (BlackBerry)	Deep Learning	Malware detection using behavioral analysis.	- Identified zero-day malware. - Reduced reliance	- High computational cost. - Limited

			on signature-based detection.	interpretability of results.
Google's Gmail Phishing Filter	Natural Language Processing	Detection of phishing emails using content analysis.	- Reduced phishing email success rate. - Improved user awareness.	- Struggles with sophisticated spear-phishing attacks.
IBM Watson for Cybersecurity	Machine Learning & NLP	Threat intelligence and incident response automation.	- Improved threat detection accuracy. - Automated incident response.	- Requires large datasets. - High implementation cost.
Palo Alto Networks Cortex XDR	Deep Learning & Reinforcement Learning	Endpoint detection and response (EDR).	- Enhanced threat visibility. - Automated mitigation of threats.	- Complex deployment. - Requires skilled personnel for management.

One of the key advantages of NLP is its ability to understand and interpret human language. This is particularly important in the context of cybersecurity, where many threats involve social engineering tactics, such as phishing and spear-phishing. NLP algorithms can analyze the content of emails and other text-based communications to identify potential threats, even if they are disguised as legitimate communications[13].

NLP algorithms can also be used to analyze the sentiment of text, which can be useful in identifying potential insider threats. For example, an employee who is disgruntled or unhappy may be more likely to engage in malicious behavior. NLP algorithms can analyze the sentiment of an employee's communications to identify potential risks and take proactive measures to mitigate them.



AI-Driven Threat Detection Techniques

AI-driven threat detection techniques leverage the power of AI to identify and respond to cyber threats in real-time. These techniques can be used to analyze network traffic, detect malware, and identify phishing emails, among other things. In this section, we will explore some of the most common AI-driven threat detection techniques and their effectiveness in enhancing cybersecurity measures[14].

Anomaly Detection

Anomaly detection is a technique that involves identifying patterns in data that deviate from the norm. In the context of cybersecurity, anomaly detection can be used to identify unusual network traffic, which may

indicate a potential cyber threat. AI-driven anomaly detection techniques can analyze large volumes of network traffic in real-time, allowing for faster and more accurate threat detection[15].

One of the key advantages of AI-driven anomaly detection is its ability to detect previously unknown threats. Traditional anomaly detection techniques often rely on rule-based systems, which can be limited in their ability to detect new and emerging threats. AI-driven anomaly detection, on the other hand, can continuously learn and adapt to new threats, making it a more effective tool for threat detection.

AI-driven anomaly detection techniques can also be used to identify insider threats. Insider threats involve malicious behavior by employees or other trusted individuals within an organization. AI-driven anomaly detection can analyze the behavior of employees to identify potential risks, such as unusual access patterns or data transfers[16].

Malware Detection

Malware detection is a technique that involves identifying and neutralizing malicious software, such as viruses, worms, and ransomware. AI-driven malware detection techniques can analyze the behavior of software to identify potential threats, even if they have not been previously encountered. This is particularly important in the context of zero-day exploits, which involve vulnerabilities that are unknown to the software vendor.

One of the key advantages of AI-driven malware detection is its ability to detect polymorphic malware. Polymorphic malware is a type of malware that can change its code to evade detection by traditional security measures. AI-driven malware detection techniques can analyze the behavior of software to identify potential threats, even if the code has been altered.

AI-driven malware detection techniques can also be used to analyze the behavior of software in real-time. This allows for faster and more accurate threat detection, reducing the time it takes to identify and neutralize malware. Additionally, AI-driven malware detection techniques can be used to analyze large volumes of data, making them suitable for use in large-scale networks[17].

Phishing Detection

Phishing detection is a technique that involves identifying and neutralizing phishing emails, which are designed to trick individuals into revealing sensitive information. AI-driven phishing detection techniques can analyze the content of emails to identify potential threats, even if they are disguised as legitimate communications. This is particularly important in the context of spear-phishing, which involves targeted attacks on specific individuals or organizations.

One of the key advantages of AI-driven phishing detection is its ability to analyze the content of emails in real-time. This allows for faster and more accurate threat detection, reducing the time it takes to identify and neutralize phishing emails. Additionally, AI-driven phishing detection techniques can be used to analyze large volumes of data, making them suitable for use in large-scale networks[18].

AI-driven phishing detection techniques can also be used to analyze the behavior of users to identify potential risks. For example, if a user frequently clicks on links in emails, they may be more susceptible to phishing attacks. AI-driven phishing detection techniques can analyze the behavior of users to identify potential risks and take proactive measures to mitigate them.

AI-Driven Mitigation Techniques

AI-driven mitigation techniques leverage the power of AI to neutralize cyber threats and prevent them from causing damage. These techniques can be used to block malicious traffic, quarantine infected devices, and remediate vulnerabilities, among other things. In this section, we will explore some of the most common AI-driven mitigation techniques and their effectiveness in enhancing cybersecurity measures[19].

Automated Incident Response

Automated incident response is a technique that involves using AI to automatically respond to cyber threats in real-time. This can include blocking malicious traffic, quarantining infected devices, and remediating vulnerabilities. Automated incident response can help to reduce the time it takes to respond to cyber threats, minimizing the potential damage caused by an attack.

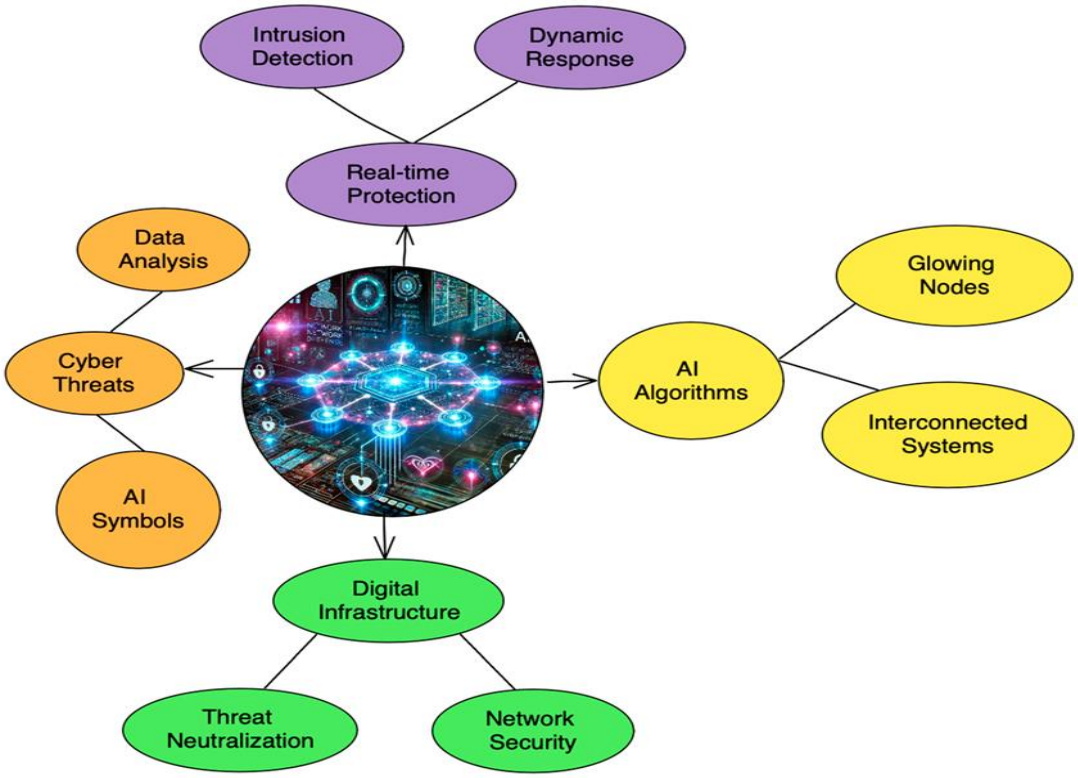
One of the key advantages of automated incident response is its ability to respond to threats in real-time. Traditional incident response techniques often involve manual intervention, which can be time-consuming and error-prone. Automated incident response, on the other hand, can respond to threats in real-time, reducing the time it takes to neutralize an attack.

Automated incident response can also be used to analyze the behavior of threats and take proactive measures to mitigate them. For example, if a particular type of malware is detected, automated incident response can analyze the behavior of the malware and take steps to prevent it from spreading. This can help to reduce the impact of an attack and prevent it from causing further damage[20].

Vulnerability Management

Vulnerability management is a technique that involves identifying and remediating vulnerabilities in a network. AI-driven vulnerability management techniques can analyze the behavior of a network to identify potential vulnerabilities, even if they have not been previously encountered. This is particularly important in the context of zero-day exploits, which involve vulnerabilities that are unknown to the software vendor[21].

One of the key advantages of AI-driven vulnerability management is its ability to analyze large volumes of data in real-time. This allows for faster and more accurate identification of vulnerabilities, reducing the time it takes to remediate them. Additionally, AI-driven vulnerability management techniques can be used to analyze the behavior of a network to identify potential risks, such as unusual access patterns or data transfers.



AI-driven vulnerability management techniques can also be used to prioritize vulnerabilities based on their potential impact. This can help to ensure that the most critical vulnerabilities are addressed first, reducing the risk of a successful cyberattack. Additionally, AI-driven vulnerability management techniques can be used to automate the remediation process, reducing the workload on cybersecurity professionals.

Threat Intelligence

Threat intelligence is a technique that involves collecting and analyzing information about potential cyber threats. AI-driven threat intelligence techniques

can analyze large volumes of data from various sources, such as social media, dark web forums, and threat feeds, to identify potential threats. This can help to provide early warning of potential attacks, allowing organizations to take proactive measures to mitigate them[22].

One of the key advantages of AI-driven threat intelligence is its ability to analyze large volumes of data in real-time. This allows for faster and more accurate identification of potential threats, reducing the time it takes to respond to them. Additionally, AI-driven threat intelligence techniques can be used to analyze the behavior of threats and take proactive measures to mitigate them[23].

AI-driven threat intelligence techniques can also be used to provide context for potential threats. For example, if a particular type of malware is detected, AI-driven threat intelligence can provide information about the origin of the malware, the tactics used by the attackers, and the potential impact of the attack. This can help to provide a more comprehensive understanding of the threat,

allowing organizations to take more effective measures to mitigate it.

Challenges and Limitations of AI in Cybersecurity

While AI has proven to be a valuable tool in enhancing cybersecurity measures, it is not without its challenges and limitations. In this section, we will explore some of the most significant challenges and limitations of AI in cybersecurity and discuss potential solutions[24].

Data Quality and Availability

One of the key challenges of AI in cybersecurity is the quality and availability of data. AI algorithms rely on large volumes of high-quality data to learn and make accurate predictions. However, in the context of cybersecurity, data can often be incomplete, inconsistent, or biased. This can lead to inaccurate predictions and false positives, reducing the effectiveness of AI-driven cybersecurity measures.

One potential solution to this challenge is to improve the quality and availability of data. This can be achieved by implementing data governance practices, such as data cleansing and data normalization, to ensure that data is accurate and consistent. Additionally, organizations can invest in data collection and storage infrastructure to ensure that they have access to large volumes of high-quality data[25].

Adversarial Attacks

Another significant challenge of AI in cybersecurity is the risk of adversarial attacks. Adversarial attacks involve manipulating the input data to an AI algorithm in order to cause it to make incorrect predictions. In the context of cybersecurity, adversarial attacks can be used to bypass AI-driven security measures, allowing cybercriminals to carry out successful attacks.

One potential solution to this challenge is to develop more robust AI algorithms that are resistant to adversarial attacks. This can be achieved by implementing techniques such as adversarial training, which involves training AI algorithms on adversarial examples to improve their robustness. Additionally, organizations can implement multi-layered security measures to reduce the risk of successful adversarial attacks[26].

Ethical and Legal Considerations

The use of AI in cybersecurity also raises several ethical and legal considerations. For example, the use of AI-driven surveillance techniques to monitor employee behavior can raise concerns about privacy and civil liberties. Additionally, the use of AI-driven decision-making in cybersecurity can raise concerns about accountability and transparency.

One potential solution to these challenges is to develop ethical and legal frameworks for the use of AI in cybersecurity. This can include guidelines for the responsible use of AI, as well as regulations to ensure that AI-driven cybersecurity measures are transparent and accountable. Additionally, organizations can implement privacy-preserving techniques, such as differential privacy, to protect the privacy of individuals while still leveraging the power of AI.

Future Research Directions

While AI has proven to be a valuable tool in enhancing cybersecurity measures, there is still much work to be done in this field. In this section, we will explore some potential future research directions for the use of AI in cybersecurity[27].

Explainable AI

One potential future research direction is the development of explainable AI techniques. Explainable AI involves developing AI algorithms that can provide clear and understandable explanations for their predictions and decisions. This is particularly important in the context of cybersecurity, where the decisions made by AI algorithms can have significant consequences.

Explainable AI can help to improve the transparency and accountability of AI-driven cybersecurity measures, making it easier for organizations to understand and trust the decisions made by AI algorithms. Additionally, explainable AI can help to identify potential biases and errors in AI algorithms, improving their accuracy and effectiveness[28].

Federated Learning

Another potential future research direction is the development of federated learning techniques. Federated learning involves training AI algorithms on decentralized data sources, such as edge devices, without transferring the data to a central server. This can help to improve the privacy and security of data, as well as reduce the risk of data breaches.

Federated learning can be particularly useful in the context of cybersecurity, where data is often sensitive and confidential. By training AI algorithms on decentralized data sources, organizations can leverage the power of AI while still protecting the privacy and security of their data. Additionally, federated learning can help to improve the scalability of AI-driven cybersecurity measures, making them suitable for use in large-scale networks[29].

Quantum Computing

Quantum computing is another potential future research direction for the use of AI in cybersecurity. Quantum

computing involves the use of quantum-mechanical phenomena, such as superposition and entanglement, to perform computations. Quantum computing has the potential to revolutionize the field of cybersecurity, as it can be used to develop more powerful encryption algorithms and break existing encryption algorithms[30].

One potential application of quantum computing in cybersecurity is the development of quantum-resistant encryption algorithms. These algorithms can help to protect against the threat of quantum computing, which has the potential to break existing encryption algorithms. Additionally, quantum computing can be used to develop more powerful AI algorithms, improving their accuracy and effectiveness in detecting and mitigating cyber threats[31].

Conclusion

The rapid evolution of cyber threats has necessitated the development of advanced techniques for threat detection and mitigation. Artificial Intelligence (AI) has emerged as a pivotal tool in enhancing cybersecurity measures, offering innovative solutions for identifying and neutralizing cyber threats. This article has provided a comprehensive review of the role of AI in cybersecurity, focusing on its application in threat detection and mitigation[32].

We have explored various AI techniques, including machine learning, deep learning, and natural language processing, and their effectiveness in enhancing cybersecurity measures. We have also discussed the challenges and limitations of AI in cybersecurity, as well as potential future research directions. While AI has proven to be a valuable tool in the fight against cyber threats, there is still much work to be done in this field[33].

References

[1] T. Satyapanich, F. Ferraro, and T. Finin, "CASIE: Extracting cybersecurity event information from text," *Proc. Conf. AAAI Artif. Intell.*, vol. 34, no. 05, pp. 8749–8757, Apr. 2020.

[2] C. Yinka-Banjo and O.-A. Ugot, "A review of generative adversarial networks and its application in cybersecurity," *Artif. Intell. Rev.*, vol. 53, no. 3, pp. 1721–1736, Mar. 2020.

[3] P. Radanliev *et al.*, "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains," *Cybersecurity*, vol. 3, no. 1, Dec. 2020.

[4] N. Kseniia and A. Minbaleev, "Legal support of cybersecurity in the field of application of artificial intelligence technology," in *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, Yaroslavl, Russia, 2020.

[5] R. Damoose, "A framework for disclosing DoD artificial intelligence-based cybersecurity product information," in *Proceedings of the 7th International Conference on Management of e-Commerce and e-Government*, Jeju Island Republic of Korea, 2020.

[6] G. Stamatescu, I. Stamatescu, N. Arghira, and I. Fagarasan, "Cybersecurity Perspectives for Smart Building Automation Systems," in *2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Bucharest, Romania, 2020.

[7] M. J. Guitton, "Cybersecurity, social engineering, artificial intelligence, technological addictions: Societal challenges for the coming decade," *Comput. Human Behav.*, vol. 107, no. 106307, p. 106307, Jun. 2020.

[8] A. Massaro, G. Panarosa, N. Savino, S. Buonopane, and A. Galiano, "Advanced multimedia platform based on big data and artificial intelligence improving cybersecurity," *Int. J. Netw. Secur. Appl.*, vol. 12, no. 3, pp. 23–37, May 2020.

[9] M. Blowers and J. Williams, "Artificial intelligence presents new challenges in cybersecurity," in *Disruptive Technologies in Information Sciences IV*, Online Only, United States, 2020.

[10] S. Samtani, M. Kantarcioglu, and H. Chen, "Trailblazing the artificial Intelligence for cybersecurity discipline," *ACM Trans. Manag. Inf. Syst.*, vol. 11, no. 4, pp. 1–19, Dec. 2020.

[11] G. Kabanda, "Performance of Machine Learning and other Artificial Intelligence paradigms in Cybersecurity," *Orient. J. Comput. Sci. Technol.*, vol. 13, no. 1, pp. 1–21, May 2020.

[12] H. Chaudhary, A. Detroja, P. Prajapati, and P. Shah, "A review of various challenges in cybersecurity using Artificial Intelligence," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, Thoothukudi, India, 2020.

[13] N. Scarpato, N. D. Cilia, and M. Romano, "Reachability matrix ontology: A cybersecurity ontology," *Appl. Artif. Intell.*, vol. 33, no. 7, pp. 643–655, Jun. 2019.

[14] P. Sornsuwit and S. Jaiyen, "A new hybrid machine learning for cybersecurity threat detection based on adaptive boosting," *Appl. Artif. Intell.*, vol. 33, no. 5, pp. 462–482, Apr. 2019.

[15] S. Haykin, "Artificial intelligence communicates with cognitive dynamic system for cybersecurity," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 3, pp. 463–475, Sep. 2019.

[16] M. Taddeo, "Three ethical challenges of applications of artificial intelligence in cybersecurity," *Minds Mach. (Dordr.)*, vol. 29, no. 2, pp. 187–191, Jun. 2019.

[17] M. Taddeo, T. McCutcheon, and L. Floridi, "Trusting artificial intelligence in cybersecurity is a double-edged sword," *Nat. Mach. Intell.*, vol. 1, no. 12, pp. 557–560, Nov. 2019.

[18] G. W. Romney, J. Guymon, M. D. Romney, and D. A. Carlson, "Curriculum for Hands-on Artificial Intelligence Cybersecurity," in *2019 18th International Conference on Information Technology Based Higher Education and Training (ITHET)*, Magdeburg, Germany, 2019.

[19] K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, and T. Tran, "Grand challenge: Applying artificial intelligence and

machine learning to cybersecurity," *Computer (Long Beach Calif.)*, vol. 52, no. 12, pp. 45–52, Dec. 2019.

[20] I. Chomiak-Orsa, A. Rot, and B. Blaicke, "Artificial intelligence in cybersecurity: The use of AI along the cyber kill chain," in *Computational Collective Intelligence*, Cham: Springer International Publishing, 2019, pp. 406–416.

[21] X. Wang, B. An, and H. Chan, "Who should pay the cost: A game-theoretic model for government subsidized investments to improve national cybersecurity," in *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence*, Macao, China, 2019.

[22] I. Ilhan and M. Karakose, "Requirement analysis for cybersecurity solutions in industry 4.0 platforms," in *2019 International Artificial Intelligence and Data Processing Symposium (IDAP)*, Malatya, Turkey, 2019.

[23] G. I. Simari, "From data to knowledge engineering for cybersecurity," in *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence*, Macao, China, 2019.

[24] J. Yoon, S. Hwang, D.-R. Lee, and N. Kang, "Operation techniques and hydrological applications of X-band dual-polarization radar for monitoring flash flood in metropolitan area," *Korean Soc. Hazard Mitig.*, vol. 20, no. 2, pp. 25–33, Apr. 2020.

[25] P. A. Kowalski, K. Sapała, and W. Warchałowski, "PM10 forecasting through applying convolution neural network techniques," *Int. J. Environ. Impacts Manag. Mitig. Recovery*, vol. 3, no. 1, pp. 31–43, Jan. 2020.

[26] M. S. Alam, B. Selim, G. Kaddoum, and B. L. Agba, "Mitigation techniques for impulsive noise with memory modeled by a two state Markov-Gaussian process," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4079–4088, Sep. 2020.

[27] J. Son, Y. Seo, Y. Park, and G. Cho, "Temperature prediction of anti-frost layer using machine learning techniques," *Korean Soc. Hazard Mitig.*, vol. 20, no. 1, pp. 9–17, Feb. 2020.

[28] A. P. Sk and P. Kumar, "Review of power quality issues and mitigation techniques in electrical power systems," *International Journal of Engineering Technology and Management Sciences*, vol. 4, no. 5, pp. 116–120, Sep. 2020.

[29] N. Kumar, S. Nema, R. K. Nema, and D. Verma, "A state-of-the-art review on conventional, soft computing, and hybrid techniques for shading mitigation in photovoltaic applications," *Int. Trans. Electr. Energy Syst.*, vol. 30, no. 9, p. e12420, Sep. 2020.

[30] S. Parison, M. Hendel, and L. Royon, "A statistical method for quantifying the field effects of urban heat island mitigation techniques," *Urban Clim.*, vol. 33, no. 100651, p. 100651, Sep. 2020.

[31] A. Narmilan and N. Puvanitha, "Mitigation techniques for agricultural pollution by precision technologies with a focus on the Internet of Things (IoTs): A review," *Agric. Rev.*, vol. 41, no. 03, Aug. 2020.

[32] P. Tamagnone, E. Comino, and M. Rosso, "Rainwater harvesting techniques as an adaptation strategy for flood mitigation," *J. Hydrol. (Amst.)*, vol. 586, no. 124880, p. 124880, Jul. 2020.

[33] C.-N. Chen, Y. Chen, Y. Wang, T.-Y. Kuo, and H. Wang, "38-GHz CMOS linearized receiver with IM3 suppression, $P_{1\,dB}$/IP3/RR3 enhancements, and mitigation of QAM constellation diagram distortion in 5G MMW systems," *IEEE Trans. Microw. Theory Tech.*, vol. 68, no. 7, pp. 2779–2795, Jul. 2020.