JCMM Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in
e-ISSN: 3009-075X
AAN PUBLISHING

Volume 2 Issue 3

Article Number: 23064

Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era

Sarvesh Kumar [*], Upasana Gupta, Arvind Kumar Singh, and Avadh Kishore Singh

Department of Computer Science Engineering, Babu Banarasi Das University, Lucknow, Uttar pradesh, India 226028

Abstract

As we navigate the digital era of the 21st century, cyber security has grown into a pressing societal issue that requires innovative, cutting-edge solutions. In response to this pressing need, Artificial Intelligence (AI) has emerged as a revolutionary instrument, causing a paradigm shift in cyber security. AI's prowess resides in its capacity to process and analyze immense quantities of heterogeneous cyber security data, thereby facilitating the efficient completion of crucial tasks. These duties, which include threat detection, asset prioritization, and vulnerability management, are performed with a level of speed and accuracy that far exceeds human capabilities, thereby transforming our approach to cyber security. This document provides a comprehensive dissection of AI's profound impact on cyber security, as well as an in-depth analysis of how AI tools not only augment, but in many cases transcend human-mediated processes. By delving into the complexities of AI implementation within the realm of cyber security, we demonstrate the potential for AI to effectively anticipate, identify, and preempt cyber threats, empowering organizations to take a proactive stance towards digital safety. Despite these advancements, it is essential to consider the inherent limitations of AI. We emphasize the need for sustained human oversight and intervention to ensure that cyber security measures are proportionate and effective. Importantly, we address potential ethical concerns and emphasize the significance of robust governance structures for the responsible and transparent use of artificial intelligence in cyber security. This paper clarifies the transformative role of AI in reshaping cyber security strategies, thereby contributing to a safer, more secure digital future. In doing so, it sets the groundwork for further exploration and discussion on the use of AI in cyber security, a discussion that is becoming increasingly important as we continue to move deeper into the digital age.

Keywords: Artificial Intelligence; Cyber Security; Vulnerability Management; Control Distribution; Human Senses Mimicry

1 Introduction

The rise of the digital era has revolutionized numerous industries across the globe, including healthcare, finance, and education [1]. Nonetheless, this digital transformation has spawned numerous challenges, especially in cyber security [2–4]. While essential, conventional protection measures such as antivirus software and firewalls are proving insufficient in the face of an ever-changing and increasingly complex cyber threat landscape. The need for dynamic, robust, and effective cyber security solutions has never been greater. The introduction and incorporation of Artificial Intelligence (AI) in cyber security has emerged as a potential game-changer in this context [5–7]. Artificial Intelligence (AI), characterized by its capacity to imitate and potentially surpass human cognitive functions, has been identified as a crucial tool for bolstering cyber security. Using complex algorithms, AI can extract patterns from vast datasets, adapt to new information, and predict with unprecedented accuracy [8, 9]. Its speed, accuracy, and ability to identify novel cyber threats vastly surpass those of conventional security systems, making it an increasingly vital component of cyber security protocols [10–12].

[*] Corresponding author: kr.sarvi91@gmail.com

Received: 06 July 2023; **Revised:** 25 July 2023; **Accepted:** 29 July 2023; **Published:** 31 August 2023

DOI: 10.57159/gadl.jcmm.2.3.23064.

This introductory section lays the groundwork for the article's exhaustive examination of AI's role in cyber security. Further in this article, the investigation begins by elucidating the current cyber security landscape, emphasizing the diverse nature of current threats and the traditional cyber security measures used to combat them. The section then transitions into an in-depth discussion of how AI techniques, specifically machine learning, deep learning, and natural language processing, are used to enhance cyber security frameworks. In the subsequent sections, we will investigate specific AI applications in cyber security. Real-world examples, such as Symantec's Targeted Attack Analytics (TAA) and Sophos' Intercept X, demonstrate artificial intelligence's tangible impact on enhancing cyber security practices. However, as AI and cyber security become increasingly intertwined, we must be cognizant of the potential pitfalls that AI may introduce. Cyber adversaries may employ AI to execute increasingly sophisticated cyber attacks, posing new cyber security challenges. These escalating challenges necessitate the establishment of stringent ethical frameworks to govern the use of AI in cyber security, as discussed in the following section. The article concludes with a look ahead, predicting how the ongoing development of AI technologies will affect cyber security in the coming years and vice versa. This mini-review aims to provide an overview of AI's potential to enhance cyber security and emphasize the need for circumspect and responsible AI deployment. Through thorough analysis, we hope to cast light on a future in which AI, when used judiciously, can radically alter the cyber security landscape.

2 The Paradigm Shift: Artificial Intelligence in cyber security

AI has emerged as a strategic game-changer in the field of cyber security, radically reshaping traditional threat detection, vulnerability management, and network security processes [13]. This section clarifies AI's transformative role in these domains, highlighting its significant cyber security-revolutionizing strides. Figure 1 represents the possible taxonomy of AI techniques in the cyber security domain.

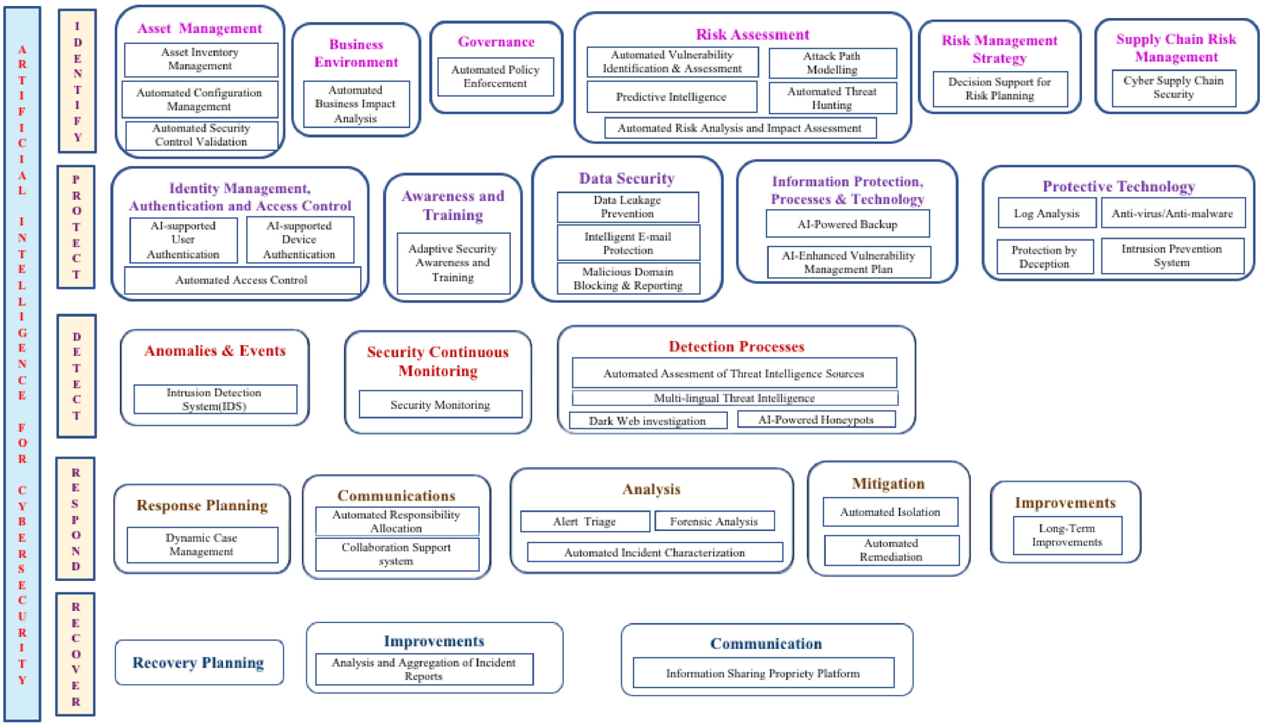
ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY
IDENTIFY
Asset Management
Asset Inventory Management
Automated Configuration Management
Automated Security Control Validation
Business Environment
Automated Business Impact Analysis
Governance
Automated Policy Enforcement
Risk Assessment
Automated Vulnerability Identification & Assessment
Attack Path Modelling
Predictive Intelligence
Automated Threat Hunting
Automated Risk Analysis and Impact Assessment
Risk Management Strategy
Decision Support for Risk Planning
Supply Chain Risk Management
Cyber Supply Chain Security
PROTECT
Identity Management, Authentication and Access Control
AI-supported User Authentication
AI-supported Device Authentication
Automated Access Control
Awareness and Training
Adaptive Security Awareness and Training
Data Security
Data Leakage Prevention
Intelligent E-mail Protection
Malicious Domain Blocking & Reporting
Information Protection, Processes & Technology
AI-Powered Backup
AI-Enhanced Vulnerability Management Plan
Protective Technology
Log Analysis
Anti-virus/Anti-malware
Protection by Deception
Intrusion Prevention System
DETECT
Anomalies & Events
Intrusion Detection System(IDS)
Security Continuous Monitoring
Security Monitoring
Detection Processes
Automated Assesment of Threat Intelligence Sources
Multi-lingual Threat Intelligence
Dark Web investigation
AI-Powered Honeypots
RESPOND
Response Planning
Dynamic Case Management
Communications
Automated Responsibility Allocation
Collaboration Support system
Analysis
Alert Triage
Forensic Analysis
Automated Incident Characterization
Mitigation
Automated Isolation
Automated Remediation
Improvements
Long-Term Improvements
RECOVER
Recovery Planning
Improvements
Analysis and Aggregation of Incident Reports
Communication
Information Sharing Propriety Platform

Figure 1: Possible taxonomy of AI techniques in the cyber security domain [14].

2.1 Threat hunting

In the past, cyber security has extensively relied on signature-based techniques for detecting threats. These techniques effectively combat known threats by identifying recurring patterns or 'signatures' associated with particular categories of cyber-attacks [15, 16] this approach has the inherent limitation of being unable to detect and respond promptly to novel, unidentified dangers that do not match known signatures. Herein lies the utility of Artificial Intelligence (AI) power. AI revolutionizes threat hunting by leveraging its powerful predictive capabilities to improve threat detection and identification. AI's strength lies in its capacity to efficiently process and analyze immense quantities of data, recognize meaningful patterns, and eliminate irrelevant noise. This is especially advantageous in the hyper-connected world of today, where the volume of data generated exceeds the computational capacity of conventional threat-hunting techniques [17, 18]. The incorporation of behavioral analysis into AI enables a more dynamic approach to threat detection. Using this method, AI systems can process numerous endpoint data within an organization's network. This information is then used to develop exhaustive application profiles that provide a comprehensive view of normal operational patterns.

These profiles serve as a benchmark for anomaly detection in real-time, where any deviation from the norm may indicate a potential security risk [19–21]. This AI-enhanced strategy results in a significant transition from reactive to proactive cyber security. With AI, organizations can not only identify and respond to threats more quickly, but they also acquire the crucial ability to anticipate and prevent cyberattacks. This transformation results in a cyber security framework that is more robust and better equipped to manage the ever-changing cyber threat landscape [22, 23].

2.2 Vulnerability Management

In the age of digital interconnectivity, managing security vulnerabilities has become exponentially more difficult. Organizations confront an ever-increasing number of potential vulnerabilities and frequently struggle to effectively manage them. Traditional approaches to vulnerability management, which typically follow a reactive paradigm and frequently wait for high-risk vulnerabilities to be exploited before addressing them, have proven insufficient in the current cyber security environment. In this context, the function of Artificial Intelligence (AI) in vulnerability management becomes transformative. The combination of AI and Machine Learning (ML) provides a proactive and predictive approach to vulnerability management [24, 25]. User and Event Behavioral Analytics (UEBA) is a significant approach. UEBA enables AI systems to perpetually analyze and learn from the baseline activity of an organization's user accounts, endpoints, and servers. This analysis aids in the identification of aberrant behaviors that deviate from the established norm. Such deviations or anomalies may indicate the existence of zero-day attacks. Zero-day attacks exploit unknown vulnerabilities before developers are able to create and disseminate patches, making them especially dangerous [26–28]. AI and UEBA can identify these assaults considerably earlier in their lifecycle. AI enables proactive protection against potential breaches, even before vulnerabilities are disclosed and rectified to the public [29, 30]. Thus, AI can inferred to be capable of revolutionizing vulnerability management. It shifts the emphasis from reactive to proactive and predictive measures. This change equips organizations with a comprehensive line of defense against cyber threats, enabling them to secure their digital assets more effectively in a cyber security landscape that is constantly evolving.

2.3 Network Security

Network security remains a critical aspect of any cyber security strategy. Two vital components of network security - creating security policies and understanding network topography - have traditionally been quite labor-intensive and time-consuming tasks [31]. However, Artificial Intelligence (AI) is reshaping this scenario, serving as a potent catalyst for efficiency and effectiveness in these areas. Security policies play an indispensable role in network security, helping identify which network connections are legitimate and which warrant further scrutiny due to potential malicious activity. AI can significantly enhance the formulation of these policies. With AI's ability to analyze vast amounts of data and learn from patterns, it can support the creation of security policies with unprecedented precision and efficiency. This leads to a more robust security framework that proactively identifies and responds to potential threats. Equally important in network security is the understanding of network topography. This involves a deep knowledge of the organization's network, including how various applications and workloads interact with each other. AI's ability to learn from network traffic patterns can significantly simplify this task. AI can suggest a practical grouping of workloads based on their interactions and provide valuable insights to inform security policy development. In essence, AI optimizes these critical aspects of network security and frees up valuable resources. By reducing the time and effort dedicated to policy creation and topography understanding, AI enables security teams to focus more on strategic aspects of network security. This leads to a more robust security posture, better threat identification, and enhanced protection against cyber threats [32–36]. The discussed applications highlight how AI is complementing traditional cyber security strategies and progressively becoming integral to them. In the fight against increasingly sophisticated cyber threats, AI offers a much-needed edge, transforming reactive security practices into proactive defense mechanisms.

3 Navigating the Challenges and Limitations of AI in cyber security

While Artificial Intelligence (AI) stands at the forefront of innovative solutions for cyber security, it is not without its challenges and limitations. The technology's transformative potential is indisputable, but acknowledging its limitations ensures a balanced and realistic approach to its implementation.

3.1 Human adversaries and AI

Artificial Intelligence (AI) has been widely adopted as a powerful tool in cyber security due to its exceptional ability to analyze data, recognize patterns, and predict threats. However, while AI has revolutionized the field, it is essential to acknowledge that it does not render human adversaries obsolete. In fact, sophisticated cybercriminals with specialized strategies can often evade AI systems, proving that the human element in cyber security still poses a significant challenge. Firstly, human adversaries are not static threats. They are creative, intelligent, and capable of adapting their strategies, making them a persistent risk despite advanced AI defenses. They can use techniques like 'data poisoning' or 'adversarial attacks' to manipulate the learning process of AI systems.

By injecting misleading or incorrect data, they can skew the AI model's understanding and decision-making, causing it to misidentify threats or overlook vulnerabilities [37–40]. Moreover, human adversaries can also take advantage of the inherent limitations of AI systems. For instance, AI models are predominantly based on historical data. Thus, they may struggle to accurately predict or respond to completely novel attack strategies that have not been previously encountered. This is where the intuition and experience of human cyber security experts are irreplaceable [41–44]. Therefore, while AI is a potent tool for automating and enhancing many aspects of cyber security, human vigilance, expertise, and adaptability should not be undervalued. Effective cyber security requires a symbiotic relationship between AI capabilities and human oversight. After all, in the intricate and evolving landscape of cyber security threats, the human element continues to be crucial in identifying, understanding, and mitigating potential risks.

3.2 AI-powered cyber attacks

AI's growing power and sophistication is not only a boon for cyber security efforts but, paradoxically, a potential catalyst for more potent and sophisticated cyber threats. As we explore the cyber security advantages of AI, we must also be wary of its weaponization potential, particularly its capacity to fuel AI-powered cyberattacks. In the hands of a malevolent actor, AI can serve as a potent tool for automating and scaling cyber threats. With AI, cybercriminals can quickly adapt to defensive measures, execute attacks at unprecedented speeds, and exploit vulnerabilities with greater precision. AI can even enable attackers to mimic human behavior, making phishing attacks more convincing and more likely to succeed [45, 44, 46–48]. Moreover, AI can assist in crafting 'smart' malware, capable of learning from the environment it infiltrates, adjusting its strategies to avoid detection, and maximizing the damage it inflicts. This means traditional security defenses, such as signature-based malware detection, are often inadequate against these advanced threats. One such example of this emerging threat is DeepLocker, a new breed of highly targeted and evasive attack tool powered by AI and unleashed by IBM Research. DeepLocker conceals its malicious intent until it reaches a specific victim, demonstrating the potential future sophistication of malware threats [46, 47]. In essence, while AI undoubtedly enhances our defensive capabilities in the cyber security realm, it also provides adversaries with the tools to craft more sophisticated, adaptable, and damaging attacks. The emerging reality of AI-powered cyber threats underscores the need to continually evolve and improve our AI-based defenses and maintain robust human oversight.

3.3 Ethical considerations and governance

The integration of AI into the fabric of cyber security entails navigating a complex web of ethical issues and implications. Though central to its utility in threat detection and prevention, the vast analytical capabilities of AI also surface significant concerns regarding data privacy and protection. As AI systems are trained on and analyze enormous volumes of data, striking a balance between leveraging this data for cyber security and safeguarding user privacy is critical. Adding to the complexity is the 'black box' problem - the lack of transparency and interpretability in the decision-making processes of some AI models [49, 50]. As AI becomes increasingly integral to cyber security, this opacity can obfuscate accountability and complicate rectifying security breaches or failures. Moreover, the susceptibility of AI to malicious use, including the creation of AI-powered cyber threats, emphasizes the urgency of ethical considerations. Unchecked, these threats could exploit AI's power to inflict wide-ranging damage, calling for stringent ethical and regulatory controls over the use of AI in this domain. In light of these challenges, robust governance structures and regulatory frameworks are necessary to steer the ethical deployment of AI in cyber security. Such measures should enforce transparency, uphold data privacy, ensure accountability, and set out clear guidelines to mitigate the potential misuse of AI [49–51]. In this way, we can responsibly harness the potential of AI to enhance cyber security while safeguarding against its risks. Therefore, the incorporation of AI in cyber security is not a panacea but a powerful tool that brings its own complexities. Navigating these challenges necessitates a measured approach that blends AI's strengths with human oversight, ethical practices, and resilient governance.

4 Case Studies Illustrating the Role of AI in cyber security

Artificial Intelligence's potential in bolstering cyber security has been increasingly recognized and harnessed by organizations worldwide. This is evident in various real-world implementations, where AI-driven tools and solutions have been used to fortify defenses, enhance threat detection, and manage vulnerabilities. Here, we explore a few notable case studies that illuminate AI's transformative role in the realm of cyber security:

4.1 Symantec's targeted attack analytics (TAA) tool

Symantec's Targeted Attack Analytics (TAA) tool is a leading example of how artificial intelligence (AI) is being applied in the field of cyber security. This innovative tool leverages the power of AI to automatically analyze vast amounts of data and identify indicators of a security breach. TAA uses advanced AI algorithms that mimic the processes, data analysis, and functions of experienced security experts. By 'learning' from human professionals, TAA can detect targeted attacks with high accuracy [52, 53]. Figure 2 represents the working principle of the discussed TAA tool.

In 2018, TAA demonstrated its effectiveness in identifying and responding to sophisticated threats when it was crucial in combating a Dragonfly 2.0 attack. This incident showcased the tool's ability to proactively detect threats and manage incidents, significantly improving the efficiency of cyber security responses. Integrating AI in tools like TAA represents a major advancement in proactive threat detection and incident management [50]. By harnessing the power of AI, cyber security professionals are able to more effectively protect against and respond to targeted attacks, substantially boosting the overall security of their systems.

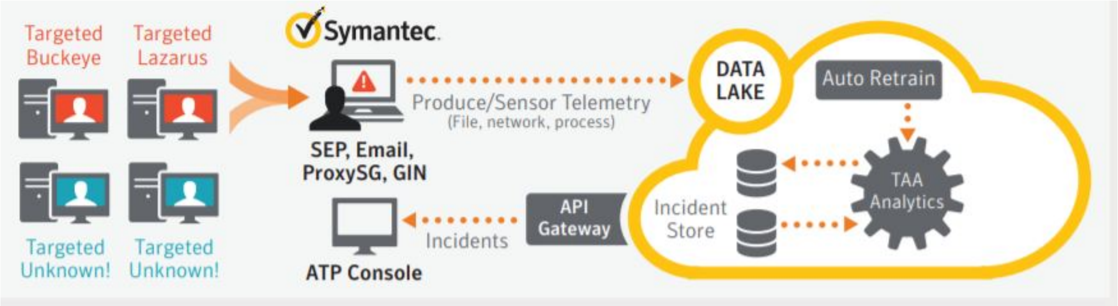

Figure 2: Working principle of the Symantec's TAA tool [54]

4.2 Sophos' intercept X

Sophos' Intercept X tool is a powerful application of artificial intelligence (AI) in the field of cyber security. This advanced tool uses deep learning neural networks, modeled after how the human brain functions, to distinguish between benign and malicious files accurately. Intercept X can analyze thousands of features from a file, conduct in-depth analysis, and determine whether the file is safe or potentially harmful within milliseconds [55–57]. Figure 3 presents the summary of the discussed Sophos' tool.

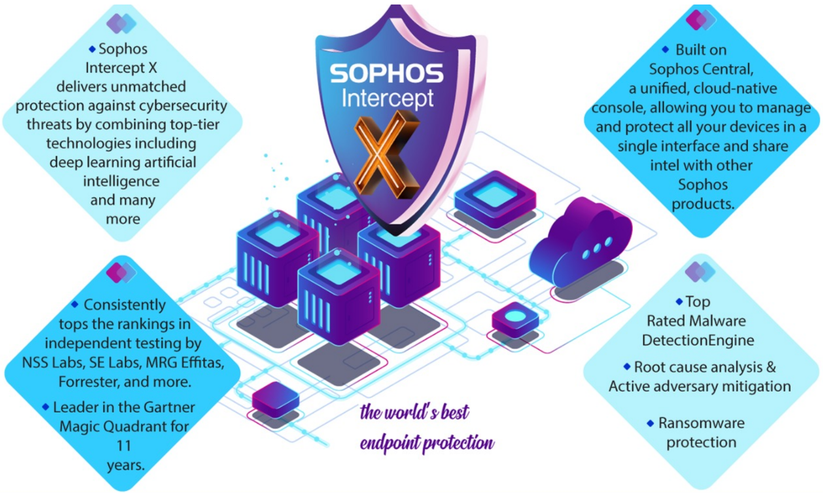
• Sophos Intercept X delivers unmatched protection against cybersecurity threats by combining top-tier technologies including deep learning artificial intelligence and many more
SOPHOS Intercept X
• Built on Sophos Central, a unified, cloud-native console, allowing you to manage and protect all your devices in a single interface and share intel with other Sophos products.
• Consistently tops the rankings in independent testing by NSS Labs, SE Labs, MRG Effitas, Forrester, and more.
• Leader in the Gartner Magic Quadrant for 11 years.
the world's best endpoint protection
• Top Rated Malware DetectionEngine
• Root cause analysis & Active adversary mitigation
• Ransomware protection

Figure 3: Summary of Sophos' intercept X tool [58].

The system is trained on real-world feedback and two-way threat intelligence, resulting in high accuracy for detecting both existing malware and zero-day threats. Additionally, Intercept X maintains a low false-positive rate, minimizing the risk of incorrectly identifying benign files as malicious. This case study reflects the potential of AI in fortifying defense mechanisms against cyber threats. By leveraging the power of AI, tools like Intercept X can bring agility and accuracy to malware detection and threat prevention, significantly improving the overall security of systems [59–61].

4.3 IBM's QRadar advisor with Watson

IBM has made significant advancements in integrating AI in cyber security with its QRadar Advisor tool. This tool uses the cognitive computing capabilities of IBM Watson to investigate potential security incidents automatically. By employing AI, the QRadar Advisor can assist security analysts in assessing threat incidents and reduce the risk of overlooking significant threats. In this case, The application of AI improves efficiency and enhances the accuracy of threat detection and response. Using advanced AI algorithms, the QRadar Advisor can quickly analyze large amounts of data and identify potential threats with high accuracy. This ultimately strengthens an organization's cyber security infrastructure by providing security analysts with powerful tools to detect and respond to cyber threats [62, 63, 15]. Figure 4 represents the three stages involved in the working of the discussed IBM tool.

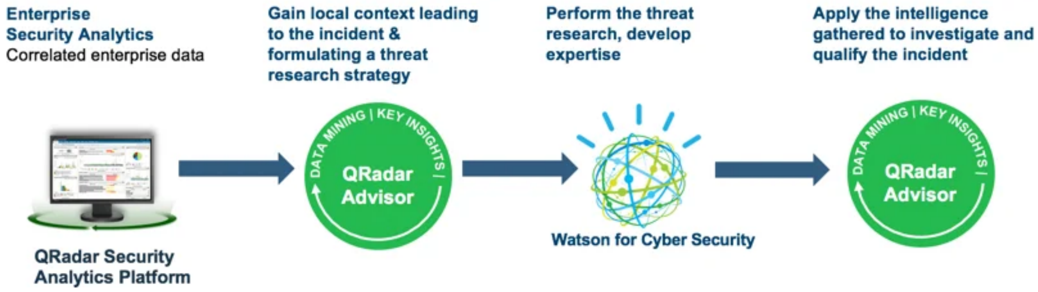
Enterprise Security Analytics
Correlated enterprise data
Gain local context leading to the incident & formulating a threat research strategy
Perform the threat research, develop expertise
Apply the intelligence gathered to investigate and qualify the incident
QRadar Advisor
DATA MINING | KEY INSIGHTS |
Watson for Cyber Security
QRadar Advisor
QRadar Security Analytics Platform

Figure 4: Stages involved in the working of IBM's QRadar advisor with Watson [64].

4.4 DeepLocker

While AI has been used to improve cyber security, it has also been used maliciously, as seen in the creation of DeepLocker - a new form of AI-powered malware. Unlike traditional malware, DeepLocker can conceal its malicious intent until it reaches a specific victim, making it incredibly difficult to detect and counter. This advanced malware uses AI and indicators such as facial recognition and geolocation to identify its target accurately. This case highlights the double-edged nature of AI in cyber security. While AI can be used to improve defenses against cyber threats, it can also be used to create advanced malware that is difficult to detect and counter. This underscores the importance of continuous advancement in AI-powered cyber security tools and measures to avoid malicious uses of AI [65–67]. Figure 5 depicts the overview of the discussed Deeplocker malware.

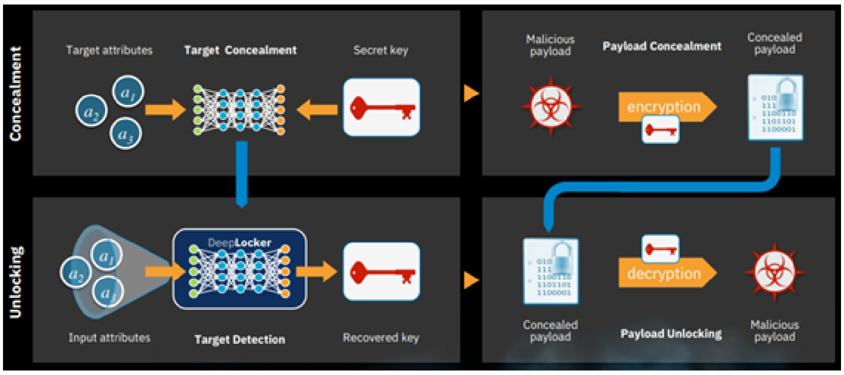

Figure 5: Process flow of deeplocker AI malware [68]

These case studies demonstrate that AI, when applied effectively, can greatly enhance cyber security. However, as seen in the DeepLocker instance, it also emphasizes the necessity of keeping pace with the evolving threat landscape where AI itself could be weaponized. From automating the detection of complex threats to learning from real-time data for proactive defense, AI is becoming a cornerstone in shaping robust and resilient cyber security strategies.

5 Future Trends and Predictions in AI and cyber security

The trajectory of Artificial Intelligence (AI) in cyber security is steeply upward, propelled by advancements in technology, rising digital threats, and the pressing need for more robust, adaptive defenses. The fusion of AI and cyber security is set to reshape the cyber landscape, bringing forth transformative changes in how organizations protect their digital assets. Here we delve into future trends and predictions in this dynamic domain:

5.1 Growth in AI-Powered cyber security market

The market for AI in cyber security is expected to experience exponential growth in the near future. Recent reports have projected that the market will expand from its current value of USD 8.8 billion in 2019 to an impressive USD 38.2 billion by 2026. This growth can be attributed to several factors, including the increasing digitization of businesses and the proliferation of connected devices. As more and more businesses move their operations online, the risk of cyber attacks increases, leading to growing concerns over data privacy and security. This has fueled demand for AI-powered cyber security solutions that can help businesses protect their data and operations. In addition to these factors, significant growth opportunities are presented by the increasing demand for AI-powered solutions among Small and Medium Enterprises (SMEs). As these businesses grow and expand their online presence, they are becoming more vulnerable to cyber attacks and therefore seeking advanced cyber security solutions to protect themselves.

Additionally, the increased use of social media for business purposes has also created new vulnerabilities that AI-powered cyber security solutions can address [69–71]. Figure 6 summarizes the anticipated global growth in AI-powered cyber security market.

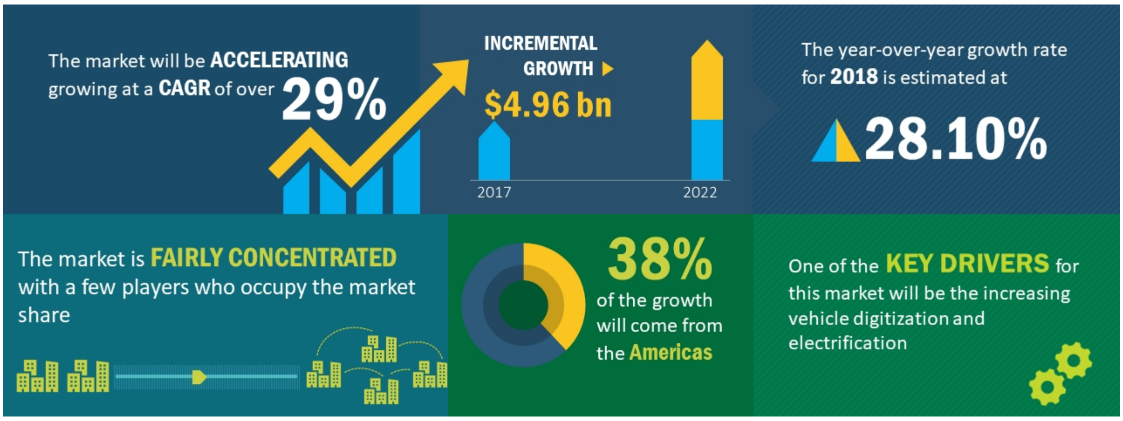

Figure 6: Anticipated global growth of AI-powered cyber security market [72].

5.2 Emergence of AI-enabled threats

As AI technology advances and becomes more sophisticated, there is a growing potential for its misuse in the form of AI-powered cyber threats. These threats can take many forms, including intelligent malware that can learn and adapt to evade detection by traditional security measures or automated phishing attacks that can accurately mimic human writing styles to trick users into revealing sensitive information. One example of this trend is the DeepLocker case, in which researchers demonstrated the potential for AI to be used to create highly targeted and evasive malware. This case highlights the critical need for advanced AI-driven defenses that can keep pace with the rapidly evolving threat landscape. As AI technology continues to advance, it is likely that we will see a surge in these types of AI-powered cyber threats. This underscores the importance of continued investment in advanced cyber security solutions to effectively defend against these emerging threats [65–67, 73, 74]. Figure 7 summarizes the various possible threats that might be posed by the emerging AI.

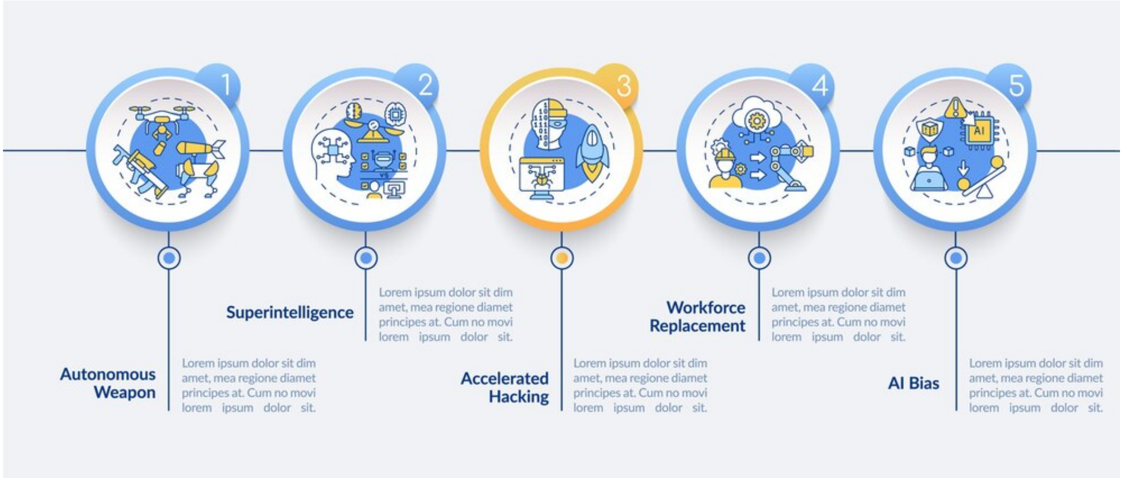
1
2
3
4
5
Autonomous Weapon
Superintelligence
Accelerated Hacking
Workforce Replacement
AI Bias
Lorem ipsum dolor sit dim amet, mea regione diamet principes at. Cum no movi lorem ipsum dolor sit.

Figure 7: Possible threats concerned with the emergence of AI [75].

5.3 Integration of AI and other emerging technologies

In the coming years, we will likely see a deeper integration of AI with other emerging technologies, such as blockchain and the Internet of Things (IoT), to enhance cyber security. These technologies have the potential to work together in powerful ways to create more secure systems and networks. For example, AI and blockchain could be combined to create decentralized systems that are more resistant to cyber attacks. Blockchain technology allows for creating secure, tamper-proof records that can be distributed across a network, making it difficult for attackers to compromise the system. Integrating AI into these systems makes it possible to create intelligent, self-healing networks that can automatically detect and respond to threats [75, 73, 76]. Similarly, AI can also help monitor and secure the vast networks of devices that make up the IoT. With billions of connected devices worldwide, it is becoming increasingly difficult to ensure that these devices are secure and not being used as entry points for cyber attacks. By integrating AI into these networks, it would be possible to automatically monitor device behavior and detect any anomalies indicating a potential security threat [77–82].

5.4 AI-powered automation in cyber security

AI technology is playing an increasingly important role in driving automation in the field of cyber security. By automating many of the routine and mundane tasks associated with cyber security, AI enables security personnel to focus on more strategic aspects of their work, such as threat analysis and incident response. One area where AI has a significant impact is in the automation of threat detection. Using advanced machine learning algorithms, AI-powered tools can automatically analyze vast amounts of data to identify potential security threats. This can help security teams to detect and respond to emerging threats quickly, reducing the risk of a successful cyber attack. In addition to threat detection, AI is also being used to automate other aspects of cyber security, such as incident response and vulnerability management. For example, AI-powered tools can automatically analyze security incidents to determine the most appropriate response or automatically scan systems for vulnerabilities and suggest remediation actions [44, 79, 83].

5.5 Greater emphasis on AI governance in cyber security

As AI technology continues to play a growing role in the field of cyber security, there is an increasing need for ethical and transparent AI practices. This will require organizations to establish robust AI governance frameworks to ensure that AI is being used ethically and responsibly, and to mitigate any potential risks associated with its use. AI governance refers to the policies, processes, and practices put in place to ensure that AI is being used in a way consistent with an organization's values and ethical principles. This can include measures such as transparency and explainability, which help ensure that AI systems are making decisions in a way that human users can understand and scrutinize. In the context of cyber security, AI governance is particularly important because of the potential risks associated with the misuse of AI technology. For example, if an AI system is not properly governed, it could be used to carry out cyber attacks or other malicious activities. To mitigate these risks, organizations must establish robust AI governance frameworks that include regular audits and risk assessments [84–86]. From the disucussion so far, it can be infered that the future of AI in cyber security is laden with both enormous potential and significant challenges. As we embrace this promising future, the focus must be on harnessing AI's power responsibly and ethically, building robust defenses, and staying vigilant of the evolving threat landscape. The constant interplay between advancing AI capabilities and emerging threats necessitates a future-proof cyber security strategy – one that continuously evolves, learns, and adapts.

6 Conclusion

The advent of Artificial Intelligence (AI) has ushered in a new era of cyber security, opening up unprecedented avenues for combating the escalating threat landscape. AI's capability to learn, adapt, and counteract cyber threats has demonstrated its substantial potential as an indispensable asset within cyber security arsenals. However, it is essential to recognize that this is only the dawn of AI's journey within the realm of cyber security. There are vast uncharted territories yet to be explored, understood, and mastered. The relentless evolution of cyber threats necessitates an equally dynamic response, which AI is well-positioned to provide. Yet, the utilization of AI in isolation may not fully address the complexity and diversity of the cyber threats we face today. The future of effective cyber security lies in a symbiotic integration of AI's speed and scalability with human expertise's creativity, intuition, and ethical judgment. This fusion of human and machine intelligence will provide a more holistic approach to identifying, responding to, and preempting cyber threats. Furthermore, as we leverage AI's transformative potential, it is paramount to maintain a focus on the ethical implications of its use. The governance of AI in cyber security must be marked by transparency, accountability, and inclusivity, thereby ensuring its responsible application. In conclusion, the revolution of AI in cyber security is underway. With continued research, responsible governance, and ethical use, AI's transformative potential can be harnessed to its fullest extent, ultimately guiding us towards a safer and more secure digital future. While challenges lie ahead, the potential benefits of AI in cyber security are immense, promising a proactive and adaptable approach to secure our increasingly interconnected world.

Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Declaration

This research did not receive any grants from governmental, private, or nonprofit funding bodies.

Author Contribution

Sarvesh Kumar: Conceptualization, Methodology, Supervision, Writing - review and editing. **Upasana Gupta**: Investigation, Visualization, Writing - original draft. **Arvind Kumar Singh**: Investigation, Visualization, Writing - original draft. **Avadh Kishore Singh**: Resources, Investigation, Visualization, Writing - original draft.

References

[1] A. Kish, “Machine Learning: A Review of Methods and Applications,” *Researchgate.Net*, 2018.

[2] P. Liu and C. Lu, “Strategic analysis and development plan design on digital transformation in the energy industry: A global perspective,” *International Journal of Energy Research*, vol. 45, pp. 19657–19670, nov 2021.

[3] J. B. Schmitt, A. Goldmann, S. T. Simon, and C. Bieber, “Conception and Interpretation of Interdisciplinarity in Research Practice: Findings from Group Discussions in the Emerging Field of Digital Transformation,” *Minerva*, vol. 61, pp. 199–220, jun 2023.

[4] A. Modi, B. Kishore, D. K. Shetty, V. P. Sharma, S. Ibrahim, R. Hunain, N. Usman, S. G. Nayak, S. Kumar, and R. Paul, “Role of Artificial Intelligence in Detecting Colonic Polyps during Intestinal Endoscopy,” *Engineered Science*, vol. 20, pp. 23–30, 2022.

[5] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, “Security issues in cloud environments: a survey,” *International Journal of Information Security*, vol. 13, pp. 113–170, apr 2014.

[6] V. Mullet, P. Sondi, and E. Ramat, “A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0,” *IEEE Access*, vol. 9, pp. 23235–23263, 2021.

[7] B. Shin and P. B. Lowry, “A review and theoretical explanation of the ‘Cyberthreat-Intelligence (CTI) capability’ that needs to be fostered in information security practitioners and how this can be accomplished,” *Computers & Security*, vol. 92, p. 101761, may 2020.

[8] M. Naveed Uddin, “Cognitive science and artificial intelligence: simulating the human mind and its complexity,” *Cognitive Computation and Systems*, vol. 1, pp. 113–116, dec 2019.

[9] P. Mikalef and M. Gupta, “Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance,” *Information & Management*, vol. 58, p. 103434, apr 2021.

[10] A. Kumar, M. Rahmath, Y. Raju, S. Reddy Vulapula, B. R. Prathap, M. M. Hassan, M. A. Mohamed, and S. A. Asakipaam, “Enhanced Secure Technique for Detecting Cyber Attacks Using Artificial Intelligence and Optimal IoT,” *Security and Communication Networks*, vol. 2022, pp. 1–13, jul 2022.

[11] R. Trifonov, O. Nakov, and V. Mladenov, “Artificial Intelligence in Cyber Threats Intelligence,” in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, pp. 1–4, IEEE, dec 2018.

[12] A. Amarasinghe, W. Wijesinghe, D. Nirmana, A. Jayakody, and A. Priyankara, “AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System,” in *2019 International Conference on Advancements in Computing (ICAC)*, pp. 363–368, IEEE, dec 2019.

[13] R. Gruetzemacher and J. Whittlestone, “The transformative potential of artificial intelligence,” *Futures*, vol. 135, p. 102884, jan 2022.

[14] R. Kaur, D. Gabrijelčič, and T. Klobučar, “Artificial intelligence for cybersecurity: Literature review and future research directions,” *Information Fusion*, vol. 97, p. 101804, sep 2023.

[15] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, “Weaponized AI for cyber attacks,” *Journal of Information Security and Applications*, vol. 57, 2021.

[16] S. C. Pallaprolu, J. M. Namayanja, V. P. Janeja, and C. T. S. Adithya, “Label propagation in big data to detect remote access Trojans,” in *2016 IEEE International Conference on Big Data (Big Data)*, pp. 3539–3547, IEEE, dec 2016.

[17] A. Syrowatka, M. Kuznetsova, A. Alsubai, A. L. Beckman, P. A. Bain, K. J. T. Craig, J. Hu, G. P. Jackson, K. Rhee, and D. W. Bates, “Leveraging artificial intelligence for pandemic preparedness and response: a scoping review to identify key use cases,” *npj Digital Medicine*, vol. 4, p. 96, jun 2021.

[18] M. Ebrahimi, J. F. Nunamaker, and H. Chen, “Semi-Supervised Cyber Threat Identification in Dark Net Markets: A Transductive and Deep Learning Approach,” *Journal of Management Information Systems*, vol. 37, pp. 694–722, jul 2020.

[19] Y. Xu, X. Liu, X. Cao, C. Huang, E. Liu, S. Qian, X. Liu, Y. Wu, F. Dong, C.-W. Qiu, J. Qiu, K. Hua, W. Su, J. Wu, H. Xu, Y. Han, C. Fu, Z. Yin, M. Liu, R. Roepman, S. Dietmann, M. Virta, F. Kengara, Z. Zhang, L. Zhang, T. Zhao, J. Dai, J. Yang, L. Lan, M. Luo, Z. Liu, T. An, B. Zhang, X. He, S. Cong, X. Liu, W. Zhang, J. P. Lewis, J. M. Tiedje, Q. Wang, Z. An, F. Wang, L. Zhang, T. Huang, C. Lu, Z. Cai, F. Wang, and J. Zhang, "Artificial intelligence: A powerful paradigm for scientific research," *The Innovation*, vol. 2, p. 100179, nov 2021.

[20] T. Kabudi, I. Pappas, and D. H. Olsen, "AI-enabled adaptive learning systems: A systematic mapping of the literature," *Computers and Education: Artificial Intelligence*, vol. 2, p. 100017, 2021.

[21] N. Haefner, J. Wincent, V. Parida, and O. Gassmann, "Artificial intelligence and innovation management: A review, framework, and research agenda," *Technological Forecasting and Social Change*, vol. 162, p. 120392, jan 2021.

[22] G. Banga, "Using Artificial Intelligence in Cybersecurity," *Www.Balbix.Com*, 2020.

[23] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, nov 2021.

[24] D. Perwej, S. Qamar Abbas, J. Pratap Dixit, D. N. Akhtar, and A. Kumar Jaiswal, "A Systematic Literature Review on the Cyber Security," *International Journal of Scientific Research and Management*, vol. 9, pp. 669–710, dec 2021.

[25] B. Li, Y. Feng, Z. Xiong, W. Yang, and G. Liu, "Research on AI security enhanced encryption algorithm of autonomous IoT systems," *Information Sciences*, vol. 575, pp. 379–398, oct 2021.

[26] S. R. Potula, R. Selvanambi, M. Karuppiah, and D. Pelusi, "Artificial Intelligence-Based Cyber Security Applications," pp. 343–373, 2023.

[27] M. Graham, R. Kukla, O. Mandrychenko, D. Hart, and J. Kennedy, "Developing Visualisations to Enhance an Insider Threat Product: A Case Study," in *2021 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pp. 47–57, IEEE, oct 2021.

[28] R. Dolas, "Analytic-driven decision support in cybersecurity : towards effective IP risk management decision-making process.," tech. rep., UNIVERSITY OF TWENTE, 2023.

[29] D. Schlette, "Cyber Threat Intelligence," in *Encyclopedia of Cryptography, Security and Privacy*, pp. 1–3, Berlin, Heidelberg: Springer Berlin Heidelberg, 2021.

[30] M. Ahmed, N. Moustafa, A. Barkat, and P. Haskell-Dowland, *Next-Generation Enterprise Security and Governance*. Boca Raton: CRC Press, feb 2022.

[31] M. Kaeo, "Designing Network Security," p. 745, 2003.

[32] J. Cheng, Y. Yang, X. Tang, N. Xiong, Y. Zhang, and F. Lei, "Generative adversarial networks: A literature review," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 12, pp. 4625–4647, 2020.

[33] Y. Hu, W. Kuang, Z. Qin, K. Li, J. Zhang, Y. Gao, W. Li, and K. Li, "Artificial Intelligence Security: Threats and Countermeasures," *ACM Computing Surveys*, vol. 55, no. 1, 2021.

[34] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," *SN Computer Science*, vol. 2, no. 3, 2021.

[35] M. Amrollahi, S. Hadayeghparast, H. Karimipour, F. Derakhshan, and G. Srivastava, "Enhancing network security via machine learning: Opportunities and challenges," *Handbook of Big Data Privacy*, pp. 165–189, 2020.

[36] F. Fourati and M.-S. Alouini, "Artificial intelligence for satellite communication: A review," *Intelligent and Converged Networks*, vol. 2, no. 3, pp. 213–243, 2021.

[37] O. Eigner, S. Eresheim, P. Kieseberg, L. D. Klausner, M. Pirker, T. Priebe, S. Tjoa, F. Marulli, and F. Mercaldo, "Towards resilient artificial intelligence: Survey and research issues," *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021*, pp. 536–542, 2021.

[38] S. Zhou, C. Liu, D. Ye, T. Zhu, W. Zhou, and P. S. Yu, "Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1–39, 2023.

[39] A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay, "A survey on adversarial attacks and defences," *CAAI Transactions on Intelligence Technology*, vol. 6, no. 1, pp. 25–45, 2021.

[40] F. Aloraini, A. Javed, O. Rana, and P. Burnap, "Adversarial machine learning in IoT from an insider point of view," *Journal of Information Security and Applications*, vol. 70, 2022.

[41] R. S. Sangwan, Y. Badr, and S. M. Srinivasan, "Cybersecurity for AI Systems: A Survey," *Journal of Cybersecurity and Privacy*, vol. 3, pp. 166–190, may 2023.

[42] A. Ayodeji, M. Mohamed, L. Li, A. Di Buono, I. Pierce, and H. Ahmed, “Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors,” *Progress in Nuclear Energy*, vol. 161, 2023.

[43] S. Kaviani, K. J. Han, and I. Sohn, “Adversarial attacks and defenses on AI in medical imaging informatics: A survey,” *Expert Systems with Applications*, vol. 198, 2022.

[44] N. Kaloudi and L. I. Jingyue, “The AI-based cyber threat landscape: A survey,” *ACM Computing Surveys*, vol. 53, no. 1, 2020.

[45] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, “The Emerging Threat of Ai-driven Cyber Attacks: A Review,” *Applied Artificial Intelligence*, vol. 36, dec 2022.

[46] T. C. Truong, Q. B. Diep, and I. Zelinka, “Artificial Intelligence in the Cyber Domain: Offense and Defense,” *Symmetry*, vol. 12, p. 410, mar 2020.

[47] L. Fritsch, A. Jaber, and A. Yazidi, “An Overview of Artificial Intelligence Used in Malware,” in *Communications in Computer and Information Science*, vol. 1650 CCIS, pp. 41–51, 2022.

[48] L. Fritsch, A. Jaber, and A. Yazidi, “An Overview of Artificial Intelligence Used in Malware,” *Communications in Computer and Information Science*, vol. 1650 CCIS, pp. 41–51, 2022.

[49] J. Chen, C. Su, and Z. Yan, “AI-Driven Cyber Security Analytics and Privacy Protection,” *Security and Communication Networks*, vol. 2019, 2019.

[50] B. Murdoch, “Privacy and artificial intelligence: challenges for protecting health information in a new era,” *BMC Medical Ethics*, vol. 22, no. 1, 2021.

[51] R. Blackman, “A Practical Guide to Building Ethical AI,” tech. rep., 2020.

[52] V. Liagkou, C. Stylios, L. Pappa, and A. Petunin, “Challenges and opportunities in industry 4.0 for mechatronics, artificial intelligence and cybernetics,” *Electronics (Switzerland)*, vol. 10, no. 16, 2021.

[53] Thiyagarajan P., “A Review on Cyber Security Mechanisms Using Machine and Deep Learning Algorithms,” pp. 23–41, 2019.

[54] CyberMaterial, “Symantec’s Targeted Attack analytics Tool (TAA).”

[55] T. M. Ghazal, M. K. Hasan, R. A. Zitar, N. A. Al-Dmour, W. T. Al-Sit, and S. Islam, “Cybers Security Analysis and Measurement Tools Using Machine Learning Approach,” *2022 1st International Conference on AI in Cybersecurity, ICAIC 2022*, 2022.

[56] N. Kshetri, “Economics of Artificial Intelligence in Cybersecurity,” *IT Professional*, vol. 23, no. 5, pp. 73–77, 2021.

[57] I. Abusamrah, A. Madhoun, and S. Iseed, “Next-Generation Firewall, Deep Learning Endpoint Protection and Intelligent SIEM Integration,” 2021.

[58] Sight and Sound Computers Limited, “Sophos Intercept X,” 2020.

[59] K. Hamid, M. W. Iqbal, M. Aqeel, X. Liu, and M. Arif, “Analysis of Techniques for Detection and Removal of Zero-Day Attacks (ZDA),” pp. 248–262, 2023.

[60] C. A. Teodorescu, “Perspectives and Reviews in the Development and Evolution of the Zero-Day Attacks,” *Informatica Economica*, vol. 26, no. 2/2022, pp. 46–56, 2022.

[61] A. Kapoor, A. Gupta, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, “Ransomware detection, avoidance, and mitigation scheme: A review and future directions,” *Sustainability (Switzerland)*, vol. 14, no. 1, 2022.

[62] R. Das and R. Sandhane, “Artificial Intelligence in Cyber Security,” *Journal of Physics: Conference Series*, vol. 1964, no. 4, 2021.

[63] D. Sasikala and K. Venkatesh Sharma, “Deployment of Artificial Intelligence with Bootstrapped Meta-Learning in Cyber Security,” *Journal of Trends in Computer Science and Smart Technology*, vol. 4, no. 3, pp. 139–152, 2022.

[64] V. Dheap, “IBM QRadar Advisor with Watson: Revolutionizing the Way Security Analysts Work,” tech. rep., 2017.

[65] G. Schram, “The Role of Artificial Intelligence in Cyber Operations: An Analysis of AI and Its Application to Malware-Based Cyberattacks and Proactive Cybersecurity,” *ProQuest Dissertations and Theses*, p. 49, 2021.

[66] M. Taddeo, “Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity,” *Minds and Machines*, vol. 29, no. 2, pp. 187–191, 2019.

[67] N. Yu, Z. Tuttle, C. J. Thurnau, and E. Mireku, “AI-powered GUI attack and its defensive methods,” *ACMSE 2020 - Proceedings of the 2020 ACM Southeast Conference*, pp. 79–86, 2020.

[68] T. Terada, T. Sakamoto, Y. Kokubu, A. Yamatani, I. Takaesu, R. Inoue, T. Ozawa, and T. Isayama, “DeepLocker : AI-embedded attack,” tech. rep., 2020.

[69] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, “The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review,” *Ijarcce*, vol. 11, no. 9, 2022.

[70] K. AL-Dosari, N. Fetais, and M. Kucukvar, “Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges,” *Cybernetics and Systems*, 2022.

[71] M. Macas, C. Wu, and W. Fuertes, “A survey on deep learning for cybersecurity: Progress, challenges, and opportunities,” *Computer Networks*, vol. 212, 2022.

[72] Freepik, “Possible threats concerned with the emergence of AI,” 2020.

[73] M. Malik, M. Kumar, V. Kumar, A. K. Gautam, S. Verma, S. Kumar, and D. Goyal, “High level browser security in cloud computing services from cross site scripting attacks,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 1073–1081, 2022.

[74] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digital Communications and Networks*, vol. 6, no. 2, pp. 147–156, 2020.

[75] Businesswire, “Global Artificial Intelligence-Based Cybersecurity Market 2018-2022 | Increasing Vulnerability to Cyber-Threats to Boost Growth | Technavio,” tech. rep., 2018.

[76] L. S. Nishad, R. Pandey, Akriti, S. Beniwal, J. Paliwal, and S. Kumar, “Security, privacy issues and challenges in cloud computing: A survey,” *ACM International Conference Proceeding Series*, vol. 04-05-Marc, 2016.

[77] N. K. Singh, S. K. Pandey, M. Nagalakshmi, A. A. Kumar, M. Tiwari, and S. Kumar, “Artificial Intelligence-based cloud computing for Industry 5.0,” *Proceedings - 2022 2nd International Conference on Innovative Sustainable Computational Technologies, CISCT 2022*, 2022.

[78] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, “Cyber security in IoT-based cloud computing: A comprehensive survey,” *Electronics (Switzerland)*, vol. 11, no. 1, 2022.

[79] A. Clim, “Cyber Security Beyond the Industry 4.0 Era. A Short Review on a Few Technological Promises,” *Informatica Economica*, vol. 23, no. 2/2019, pp. 34–44, 2019.

[80] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, “Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research,” *IEEE Access*, vol. 10, pp. 93104–93139, 2022.

[81] S. Kumar, B. Kumari, and A. Sharma, “A Purposed Approach from Artificial Intelligence Problems with 4 Problem Characteristics,” in *Proceedings of the 12th INDIACom*, pp. 4094–4096, 2018.

[82] S. Kumar, P. Kumar, S. Pal Singh, and A. Saxena, “A New Approach for Providing Security Mechanism in Cloud with Possible Solutions and Results,” *International Journal of Computer Applications*, vol. 67, no. 12, pp. 30–33, 2013.

[83] B. Dash, M. F. Ansari, P. Sharma, and A. Ali, “Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review,” *International Journal of Software Engineering & Applications*, vol. 13, no. 5, pp. 13–21, 2022.

[84] A. Razzaque, “Artificial Intelligence and IT Governance: A Literature Review,” *Studies in Computational Intelligence*, vol. 974, pp. 85–97, 2021.

[85] P. Henman, “Improving public services using artificial intelligence: possibilities, pitfalls, governance,” *Asia Pacific Journal of Public Administration*, vol. 42, no. 4, pp. 209–221, 2020.

[86] P. Robles and D. J. Mallinson, “Catching up with AI: Pushing toward a cohesive governance framework,” *Politics and Policy*, 2023.