GJETA

Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/

Global Journal of Engineering and Technology Advances
GJETA
eISSN:2582-5003
Global Scholar Press, INDIA

(Review Article)

Impact of AI on cybersecurity and security compliance

Adebola Folorunso [1, *], Temitope Adewumi [2], Adeola Adewa [3], Roy Okonkwo [4] and Tayo Nathaniel Olawumi [5]

[1] *School of Business, Technology and Health Care Administration Capella University, Minneapolis, MN, USA 55402.*
[2] *Department of Electrical and Computer Engineering University of Florida.*
[3] *McClure School of Emerging Communication Technologies Scripps College of Communications Ohio University Athens, USA.*
[4] *Department of Information Technology North Carolina A & T State University.*
[5] *Department of Computer Science, Ekiti State University, Ado Ekiti.*

Global Journal of Engineering and Technology Advances, 2024, 21(01), 167–184

Publication history: Received on 11 September 2024; revised on 24 October 2024; accepted on 26 October 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.21.1.0193

Abstract

Artificial Intelligence (AI) is transforming the field of cybersecurity and reshaping security compliance practices. As cyber threats become increasingly complex, AI offers powerful tools for identifying, mitigating, and preventing attacks in real-time. AI-driven systems excel at processing vast amounts of data, detecting anomalies, and identifying patterns that traditional security systems might miss. Machine learning and deep learning algorithms enhance the ability to predict potential threats, reducing response time and improving the accuracy of threat detection. These capabilities make AI a valuable asset in addressing sophisticated threats such as zero-day vulnerabilities, advanced persistent threats (APTs), and ransomware attacks. In the realm of security compliance, AI plays a pivotal role by automating routine tasks such as monitoring, auditing, and reporting. This reduces the burden on organizations to manually enforce regulatory standards, leading to more efficient compliance with frameworks like GDPR, HIPAA, and PCI-DSS. AI can continuously assess systems to ensure that they meet compliance requirements, enhancing the ability to detect and respond to violations. Furthermore, AI contributes to governance by helping organizations develop robust security policies, track compliance metrics, and streamline incident response. However, the integration of AI in cybersecurity also presents challenges, including adversarial AI, data privacy concerns, and transparency in AI decision-making processes. Additionally, AI-driven attacks are an emerging threat that necessitates further research and regulation. Despite these challenges, the future of AI in cybersecurity and compliance looks promising, with advancements in predictive analytics, quantum computing, and autonomous security systems poised to further revolutionize the field. As AI technologies evolve, they will continue to play a critical role in fortifying cybersecurity defenses and ensuring regulatory compliance across industries.

Keywords: Artificial Intelligence; Cybersecurity; Security Compliance; Review

1. Introduction

Organizations face a continuously changing array of cyber threats that are expanding in sophistication and size in today's increasingly digitalized world. Integrating cutting-edge technology like artificial intelligence (AI) into cybersecurity frameworks is becoming crucial in order to keep up with these issues. By providing improved skills for identifying, averting, and responding to cyberattacks, artificial intelligence (AI) has the potential to completely transform the cybersecurity industry (Zeadally *et al*., 2020). Furthermore, AI may be extremely helpful in automating and optimizing security compliance procedures, ensuring that businesses comply with regulations in a timely and effective manner (Yaseen, 2022). This analysis highlights the importance of AI in cybersecurity and security compliance by examining how these fields overlap with AI.

[*] Corresponding author: Adebola Folorunso

The term artificial intelligence (AI) describes how computers, especially computer systems, may simulate human intelligence processes (Alkatheiri, 2022). Learning, reasoning, solving problems, and seeing patterns are some of these processes. AI in cybersecurity refers to a broad spectrum of technologies intended to improve, automate, and optimize security protocols. AI can evaluate enormous information in real-time, discover anomalous patterns of activity, and autonomously respond to potential dangers (Bécue *et al.*, 2021). It makes it possible for cybersecurity systems to transition from a reactive posture—responding to attacks only after they occur—to a proactive one, in which possible threats are recognized and countered before they have a chance to do harm. Machine learning (ML), a subset of AI, is particularly valuable in cybersecurity because it allows systems to learn from previous incidents and improve threat detection over time (Dasgupta *et al.*, 2022). AI-based solutions are now being used for a range of cybersecurity applications, including malware detection, intrusion detection, and prevention systems (IDPS), phishing protection, and vulnerability management. By leveraging AI, organizations can enhance their ability to combat advanced threats such as zero-day attacks, which exploit unknown vulnerabilities, and advanced persistent threats (APTs), which target systems over extended periods (Challa, 2022; Mohamed *et al.*, 2022).

Security compliance refers to the process by which organizations adhere to a set of standards, regulations, and best practices designed to protect information systems and sensitive data (Hina and Dominic, 2020). These standards may be established by industry bodies, governments, or regulatory agencies to ensure that organizations implement appropriate security controls and processes. Compliance frameworks such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI-DSS) outline specific requirements for protecting data privacy, securing systems, and reporting breaches. Meeting security compliance requirements is crucial for organizations to maintain trust with stakeholders, avoid legal penalties, and prevent financial losses due to data breaches (Aslam *et al.*, 2022). However, maintaining compliance can be complex and resource-intensive, particularly for large organizations operating across multiple jurisdictions. This is where AI can significantly improve the process by automating compliance-related tasks, continuously monitoring systems for violations, and generating real-time reports for auditors and regulators (Syed and ES, 2022).

The integration of AI into cybersecurity frameworks is critical for several reasons. First, the sheer volume and complexity of cyber threats today make it increasingly difficult for human analysts and traditional security systems to keep pace (Zibak *et al.*, 2022). AI can process and analyze data at a scale and speed far beyond human capabilities, allowing organizations to detect threats that may otherwise go unnoticed. For example, AI can sift through billions of data points to identify anomalous network activity that might indicate an ongoing attack. Second, AI-driven cybersecurity solutions offer real-time threat detection and response, reducing the time it takes to neutralize attacks. This rapid response is essential for minimizing the impact of breaches and protecting sensitive data. Third, AI can enhance cybersecurity by continually learning and adapting to new attack vectors. As cybercriminals evolve their tactics, AI systems can adjust their models, improving their effectiveness over time (Maddireddy, 2021). Finally, AI is equally important for ensuring security compliance. As regulations become more stringent and the penalties for non-compliance increase, organizations must find ways to automate compliance monitoring and reporting. AI-driven tools can help organizations meet these requirements more efficiently, freeing up resources for other critical security tasks.

The goal of this review is to present a thorough examination of the ways in which AI affects cybersecurity and security compliance. It will examine the following crucial topics: First, how AI may improve threat detection and response, with particular instances of AI-powered cybersecurity systems. The second part of the evaluation will look at how AI can automate compliance operations, which can lower the complexity and expense of complying with regulations. Third, the difficulties of incorporating AI into cybersecurity will be covered, along with concerns about aggressive AI, privacy, and transparency. Organizations may better plan for the future of digital security and governance by knowing the promise and limitations of AI in cybersecurity and compliance. The conclusion will summarize the key points and offer insights into the future of AI-driven cybersecurity and compliance frameworks.

2. AI in Cybersecurity: An Overview

Cyber threats are growing more complicated as the digital landscape changes, necessitating the need for more advanced solutions for threat detection, prevention, and response. As shown in figure 1, artificial intelligence (AI) has become a potent cybersecurity solution that helps enterprises better address these issues (Jimmy, 2021). An outline of artificial intelligence's development in security systems is given, along with an examination of threat detection and prevention applications, real-time monitoring and anomaly detection, and case studies of AI-driven cybersecurity solutions.

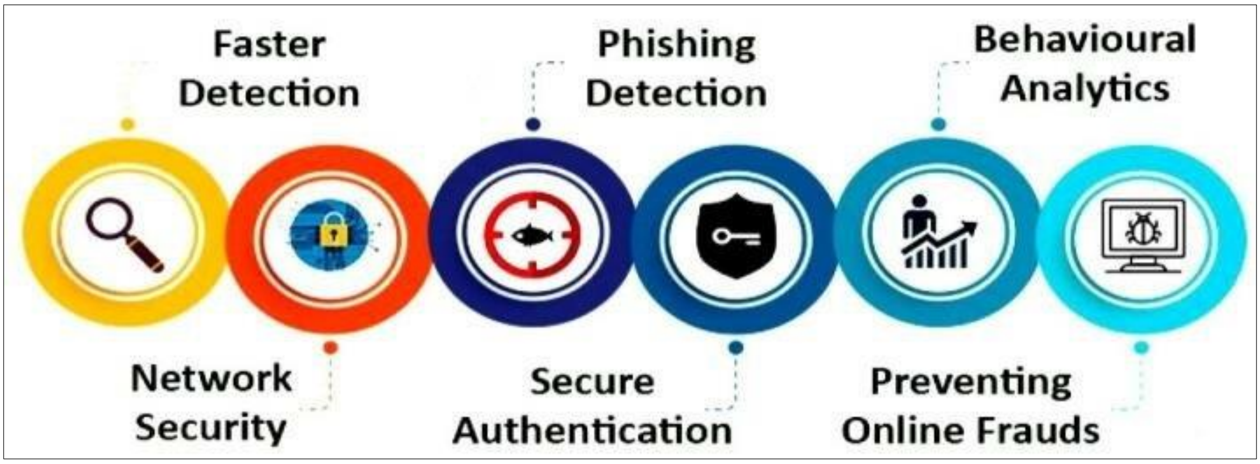

Figure 1 Application of Artificial intelligence in Cybersecurity (Narsimha *et al.*, 2022)

The integration of AI into cybersecurity has transformed how organizations approach digital security. Historically, cybersecurity relied on static, rule-based systems that were often reactive, responding to threats only after they had occurred (Calvo and Beltrán, 2022). As cyberattacks became more sophisticated, these traditional methods struggled to keep up with increasingly complex and fast-moving threats. The introduction of AI into cybersecurity marked a significant shift. AI technologies, particularly machine learning (ML) and deep learning, allowed systems to analyze vast datasets, learn from patterns, and improve over time. Instead of relying solely on pre-defined rules, AI systems could dynamically adapt to new threats. AI's ability to process massive amounts of data at high speed gave organizations the means to detect and respond to cyber threats more efficiently, creating a more proactive approach to security (Pham *et al.*, 2020).

AI is becoming essential for identifying and thwarting online threats. In order to identify anomalous activity that might indicate an attack, machine learning models are able to examine data from a variety of sources, including network traffic, user behavior, and system logs. These algorithms can detect trends that point to the existence of malware, phishing attempts, or unauthorized access by learning from past data (Tayyab *et al.*, 2022). For instance, before software developers release a patch, AI systems are able to recognize and stop zero-day vulnerabilities unknown software faults that hackers could exploit. Due to their uniqueness, these threats are difficult for traditional security systems to detect, but AI can employ predictive models to find possible weaknesses based on previous behavior. This proactive approach significantly enhances threat prevention by neutralizing risks before they can be exploited. AI also plays a critical role in threat intelligence, where it automates the collection and analysis of data from various sources to provide insights into emerging threats. This enables organizations to stay ahead of evolving cyberattack strategies and implement defenses against them in real time.

One of the most significant benefits of AI in cybersecurity is its ability to enable real-time monitoring and anomaly detection. Traditional security systems often rely on predefined rules to flag suspicious activities, which can result in missed threats or false positives. AI, however, excels at continuously analyzing data and identifying anomalies that deviate from normal behavior (Foorthuis, 2021). Anomaly detection using AI involves creating a baseline of normal system behavior and then identifying deviations that could indicate malicious activity. For example, AI can monitor network traffic and detect unusual spikes in data transfers, which could signal a distributed denial-of-service (DDoS) attack. Similarly, AI can analyze user behavior and detect unauthorized access attempts, even if they mimic normal activity patterns, such as through stolen credentials. Real-time monitoring systems powered by AI not only improve detection capabilities but also allow for faster responses to potential threats. With AI, security teams can automate incident responses, reducing the time it takes to neutralize threats. This capability is crucial for minimizing the damage caused by cyberattacks.

Several case studies demonstrate the effectiveness of AI-driven cybersecurity solutions across various sectors. One prominent example is Darktrace, a cybersecurity company that uses AI to detect, respond to, and neutralize threats in real time. Darktrace's AI-based platform analyzes network activity, detects anomalies, and autonomously mitigates threats. It has been used by organizations in industries ranging from finance to healthcare to protect against ransomware, insider threats, and advanced persistent threats (APTs). In another case, IBM's Watson for Cyber Security leverages AI to provide security analysts with insights into potential threats (Bonfanti, 2022). Watson uses natural language processing (NLP) to sift through unstructured data from security reports, blogs, and other sources, helping analysts quickly identify emerging threats and their potential impact. The time needed to examine threats is decreased with this AI-driven method, which also improves decision-making in security operations. AI-driven cybersecurity also helps the finance industry. For instance, JP Morgan Chase put in place an AI-driven fraud detection system that looks for odd patterns in consumer transaction data. This solution enhances security and improves user experience by reducing false positives and assisting in the detection of fraudulent transactions.

The evolution of AI in cybersecurity has transformed the way organizations detect, prevent, and respond to threats. AI's ability to analyze vast amounts of data, identify patterns, and learn from past incidents allows for more efficient and effective threat detection and prevention. Real-time monitoring and anomaly detection using AI further enhance the ability to identify and respond to cyber threats as they emerge (Tatineni and Mustyala, 2022). Case studies of AI-driven cybersecurity solutions, such as Darktrace and IBM Watson for Cyber Security, illustrate the tangible benefits of AI in improving security outcomes across various industries. As AI technology continues to evolve, its role in cybersecurity will become even more critical in protecting organizations from an increasingly complex cyber threat landscape.

2.1. Impact of AI on Threat Detection

Because artificial intelligence (AI) greatly improves threat detection capabilities, cybersecurity has undergone a revolution. As cyber threats continue to develop in complexity, traditional security solutions fail to keep pace with sophisticated attacks, such as zero-day vulnerabilities and advanced persistent threats (APTs) (Hejase *et al.*, 2020). AI is a crucial component of contemporary cybersecurity frameworks because of its capacity to analyze massive datasets, identify trends, and anticipate possible threats, as shown in figure 2 (Chouraik *et al.*, 2024)).

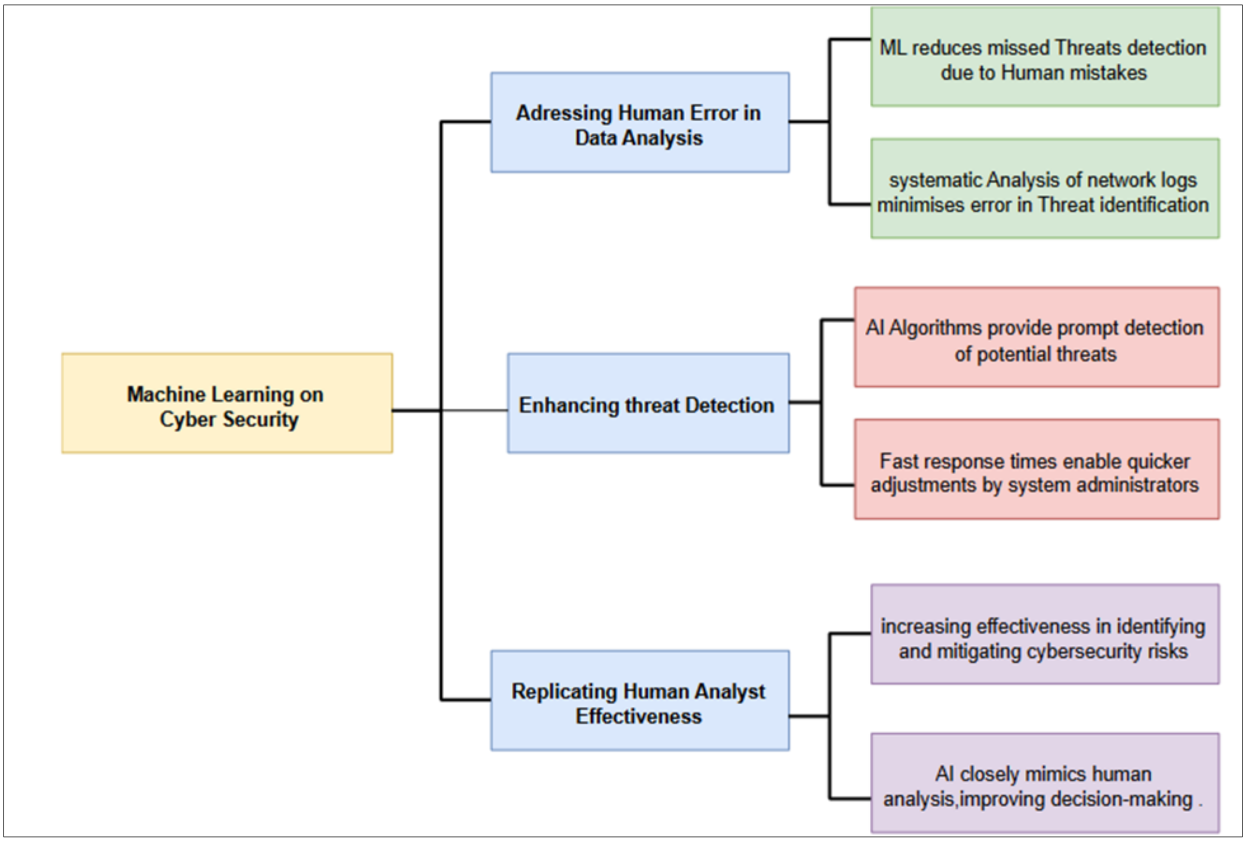
Machine Learning on Cyber Security
Adressing Human Error in Data Analysis
ML reduces missed Threats detection due to Human mistakes
systematic Analysis of network logs minimises error in Threat identification
Enhancing threat Detection
AI Algorithms provide prompt detection of potential threats
Fast response times enable quicker adjustments by system administrators
Replicating Human Analyst Effectiveness
increasing effectiveness in identifying and mitigating cybersecurity risks
AI closely mimics human analysis,improving decision-making .

Figure 2 Impact of Machine Learning (ML) on Cybersecurity (Chouraik *et al.*, 2024)

This article examines how artificial intelligence (AI) affects threat detection. It focuses on how AI can recognize complex threats, how it functions in data analysis, what kinds of AI tools are available for threat detection, and how traditional security measures fall short when compared to AI-enhanced. systems

One of the most significant contributions of AI in threat detection is its ability to identify and mitigate sophisticated cyberattacks that traditional systems often miss. Zero-day vulnerabilities, for instance, represent a major challenge for conventional security systems. These vulnerabilities are flaws in software that are unknown to the vendor, and therefore, no patch or defense is immediately available. AI can predict potential zero-day attacks by analyzing patterns in existing vulnerabilities and identifying abnormal system behavior that may indicate the exploitation of an unknown flaw. Advanced persistent threats (APTs) are another type of sophisticated attack that can go undetected by traditional methods. APTs involve prolonged and targeted cyberattacks, where attackers infiltrate systems to steal sensitive data over extended periods. AI enhances the ability to detect APTs by continuously monitoring network behavior and recognizing subtle anomalies that may signal the presence of an attacker (Nassar and Kamal, 2021). Through machine learning algorithms, AI systems can learn from past attacks and improve their detection capabilities, even as cybercriminals evolve their tactics.

The volume of data generated by organizations and their networks has grown exponentially in recent years, making it nearly impossible for human analysts and traditional systems to monitor all activities for potential threats. AI excels in processing and analyzing vast datasets in real time, allowing it to detect patterns and anomalies that might otherwise go unnoticed (Madhuri *et al.*, 2023). For example, AI can analyze network traffic, user activity logs, and system performance data to identify abnormal behavior. When unusual patterns emerge such as an unexpected spike in data transfers or unusual login locations AI systems can flag these anomalies for further investigation. Machine learning models can continuously refine their ability to detect threats by learning from historical data, adapting to new attack methods, and minimizing false positives. AI's ability to process large datasets extends beyond detecting immediate threats; it also plays a critical role in predictive threat analysis. By analyzing past incidents, AI can forecast future attacks and vulnerabilities, allowing organizations to proactively strengthen their defenses (Reddy, 2021). This predictive capability is invaluable for organizations seeking to stay ahead of increasingly sophisticated cyberattacks.

For threat detection, a number of AI tools and technologies are now in use. Cybersecurity makes extensive use of machine learning (ML) models, which are built to learn from and adjust to data trends. To detect similar patterns in new data, supervised learning models, for example, might be trained on labeled datasets containing known hazards. Conversely, unsupervised learning models are very helpful for anomaly detection since they don't need labeled data and can spot abnormalities in system behavior that might indicate hazards that weren't previously identified (Pang *et al.*, 2021). Another aspect of machine learning that has proven useful in threat detection is deep learning. Deep learning models, such as neural networks, can process complex data structures and recognize intricate patterns, making them highly effective in detecting sophisticated threats like malware and phishing attacks. These models can be trained to identify malicious code embedded in files, emails, or web pages, enabling organizations to block threats before they reach their intended targets. Specific AI-driven cybersecurity solutions, such as Darktrace and IBM Watson for Cyber Security, leverage machine learning and deep learning techniques to monitor network activity, detect threats in real time, and automate responses. Darktrace's AI platform, for example, uses unsupervised machine learning to create a baseline of normal network behavior and identify deviations that may indicate a threat. IBM Watson uses natural language processing (NLP) to analyze unstructured data, such as threat reports and blogs, to provide security analysts with insights into emerging threats (Gao *et al.*, 2021).

Traditional cybersecurity systems rely on predefined rules and signatures to detect threats. While effective against known attacks, these systems struggle to keep up with the constantly evolving nature of cyber threats. Traditional methods can only detect attacks that have been previously identified and documented, making them ineffective against zero-day vulnerabilities and novel attack vectors (Shukla, 2022). Additionally, rule-based systems are prone to producing false positives, overwhelming security teams with alerts that may not indicate real threats. In contrast, AI-enhanced systems offer a dynamic approach to threat detection. By leveraging machine learning and deep learning algorithms, AI systems can continuously learn from data, adapt to new threats, and improve their detection accuracy over time. AI reduces the likelihood of false positives by analyzing patterns and context, ensuring that only legitimate threats are flagged for investigation. Furthermore, AI-driven systems can operate in real time, providing faster threat detection and response than traditional methods, which often require manual intervention (Kaloudi and Li, 2020). Despite the clear advantages of AI in cybersecurity, challenges remain, including the need for high-quality data, the risk of adversarial AI (where attackers manipulate AI models), and concerns over the transparency and interpretability of AI decisions. However, as AI technology continues to evolve, its impact on threat detection will only grow, enabling organizations to defend against an increasingly sophisticated and persistent array of cyber threats.

Organizations may now identify and stop complex assaults like APTs and zero-day vulnerabilities thanks to AI's greatly improved threat detection skills (Al *et al.*, 2022). AI-driven systems provide a level of insight and responsiveness that traditional approaches cannot match by processing large datasets and spotting abnormalities. AI-powered solutions like Darktrace and IBM Watson, together with machine learning and deep learning, are prime examples of how AI is revolutionizing cybersecurity. Artificial intelligence (AI)-enhanced systems offer a dynamic, adaptable approach to real-time cyberattack detection and response, ushering in a new age in cybersecurity defense since traditional systems find it difficult to keep up with the constantly changing threat landscape.

2.2. AI’s Role in Incident Response

Artificial Intelligence (AI) is being used to improve incident response tactics due to the growing volume and sophistication of cyberattacks (Tao *et al*., 2021). Conventional incident response frameworks frequently depend on manual interventions, which can be cumbersome, prone to errors made by humans, and ineffective when managing intricate or large-scale threats. On the other side, artificial intelligence (AI) revolutionizes how businesses identify, address, and recover from cyber disasters by providing automation, speed, and precision. In order to reduce reaction times and human error, automation response systems, AI-powered Security Information and Event Management (SIEM) tools, and AI-enabled forensic investigation following a breach are all highlighted in this exploration of AI's role in incident response.

One of AI’s most impactful contributions to incident response is the development of automated response systems that can neutralize real-time threats. In traditional incident response, the detection of a security breach often triggers a series of manual actions analyzing the threat, deciding on the appropriate response, and executing countermeasures (Schlette *et al*., 2021). This manual process is not only time-consuming but also limits an organization’s ability to respond to fast-moving attacks, such as ransomware or distributed denial-of-service (DDoS) attacks. AI-driven automated response systems eliminate these delays by allowing immediate, machine-based responses to identified threats. For example, if AI detects an unauthorized login attempt or suspicious activity within a network, the system can automatically block access, isolate the compromised system, or flag the activity for further investigation. This capability minimizes the window of opportunity for attackers, preventing breaches from escalating and mitigating potential damage. By automating repetitive or urgent tasks, AI systems free up human analysts to focus on more complex issues and strategy. These automated systems are particularly effective in detecting and responding to low-level threats, such as malware or phishing attempts, where quick intervention is crucial. In high-risk environments, AI can even be programmed to deploy pre-defined responses to specific types of attacks, ensuring a consistent and effective response across different scenarios (Zaman *et al*., 2021).

Security Information and Event Management (SIEM) solutions are used to gather, examine, and correlate security data from all over an organization's network. Artificial Intelligence (AI) has greatly improved SIEM tool capabilities. Because of their inability to handle the massive amount of data produced by contemporary networks, traditional SIEM systems frequently need significant manual adjustment in order to recognize and address security events. A large portion of this procedure is automated by AI-powered SIEM systems using machine learning algorithms (Pulyala *et al*., 2023). Large datasets may be analyzed in real time by these technologies, which can also spot patterns and connections that might point to a security violation. AI-enhanced SIEM systems, for instance, may sort through network traffic, logs, and user behavior data to find unusual activities, including data exfiltration or unauthorized access. Once a potential threat is identified, the SIEM tool can automatically trigger an appropriate response, such as isolating affected systems, blocking suspicious IP addresses, or notifying security personnel for further action. By continuously learning from data, AI-powered SIEM tools improve their ability to detect and respond to new threats over time. This adaptability is crucial in today’s rapidly evolving cybersecurity landscape, where attackers are constantly developing new tactics to bypass conventional defenses. Additionally, AI reduces the number of false positives, ensuring that security teams are alerted only to genuine threats, thus improving overall efficiency.

AI’s ability to analyze data and execute responses in real time significantly reduces the time it takes to respond to cyber incidents. In traditional systems, the delay between detecting a threat and initiating a response can allow attackers to cause substantial damage (Azzam *et al*., 2021). By automating incident response, AI-driven systems can neutralize threats within seconds, closing this critical gap. Moreover, AI minimizes the risk of human error, a common issue in cybersecurity. Human analysts may overlook threats due to the sheer volume of data they need to process, or they may make incorrect decisions under pressure, especially during large-scale attacks. AI, on the other hand, consistently applies pre-defined rules and machine learning models to identify and respond to threats. This consistency ensures that security protocols are followed precisely, reducing the likelihood of errors that could exacerbate a breach. In addition, AI systems can scale more effectively than human teams, making them invaluable for organizations that manage vast networks or process massive amounts of data. While human analysts can become overwhelmed during a cyberattack, AI can continue to monitor and respond to multiple threats simultaneously without losing effectiveness (Whyte, 2020).

AI plays a vital role not only in responding to active threats but also in conducting forensic analysis after a breach has occurred. Following a cyberattack, it is critical to understand how the breach happened, what systems were affected, and whether the attackers left any residual threats behind. Traditionally, this post-breach analysis involves sifting through large amounts of data to reconstruct the timeline of the attack, a process that can be both time-consuming and prone to oversight. AI-enabled forensic tools streamline this process by automating data analysis and identifying key events and indicators of compromise. Machine learning algorithms can quickly correlate logs, network traffic, and system behavior to create a detailed picture of the breach. These tools can also identify any ongoing threats, such as backdoors left by the attackers, ensuring that the system is fully secured before returning to normal operations. By automating forensic analysis, AI reduces the time it takes to recover from a breach and minimizes the risk of future attacks. AI can also identify patterns in the attack that may point to a broader campaign or series of attacks, allowing organizations to prepare for similar incidents in the future (Guembe *et al*., 2022).

With automated systems that can identify and neutralize threats in real time, improved SIEM tools for better data analysis, and a dramatic reduction in response time and human error, artificial intelligence (AI) has completely changed incident response in cybersecurity. Furthermore, AI-powered forensic tools enhance post-breach investigations, guaranteeing that businesses can bounce back from cyber disasters fast and fully. AI will play an even bigger part in incident response as cyber threats continue to change, offering enterprises faster, more accurate, and more effective security solutions to help them stay ahead of more skilled attackers (Kuzlu *et al*., 2021).

2.3. AI and Predictive Security Models

Conventional security frameworks frequently react to events after they happen, which can result in serious harm and monetary loss. Artificial Intelligence (AI) has become a potent tool for creating predictive security models in order to buck this tendency (Rangaraju, 2023). These models use sophisticated analytics to manage risks, evaluate vulnerabilities, foresee cyberthreats, and put proactive security plans into action. Predictive analytics, AI-based vulnerability assessments, AI in risk management, and real-world case studies illustrating the effectiveness of predictive AI models in cybersecurity are the main topics of this exploration of the use of AI in predictive security models. Figure 3 illustrates how the swift development of cyberthreats in the field of cybersecurity calls for a change from reactive to proactive security measures (Anitha *et al*., 2022).

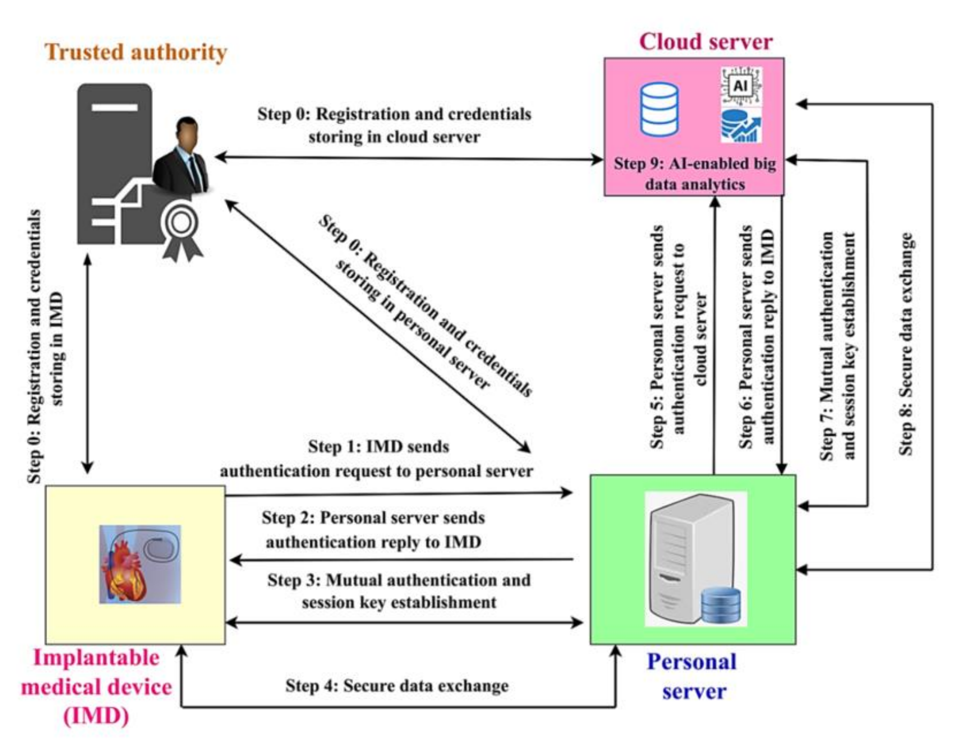
Trusted authority
Cloud server
AI
Step 0: Registration and credentials storing in cloud server
Step 9: AI-enabled big data analytics
Step 0: Registration and credentials storing in IMD
Step 0: Registration and credentials storing in personal server
Step 5: Personal server sends authentication request to cloud server
Step 6: Personal server sends authentication reply to IMD
Step 7: Mutual authentication and session key establishment
Step 8: Secure data exchange
Step 1: IMD sends authentication request to personal server
Step 2: Personal server sends authentication reply to IMD
Step 3: Mutual authentication and session key establishment
Step 4: Secure data exchange
Implantable medical device (IMD)
Personal server

Figure 3 An example of the AI-driven security model's flow (Anitha *et al*., 2022)

Predictive analytics involves the use of statistical algorithms and machine learning techniques to analyze historical data and identify patterns that can indicate future events. In cybersecurity, predictive analytics can anticipate potential cyber threats by examining data from previous attacks, user behaviors, and network traffic. This approach enables organizations to identify vulnerabilities and assess their threat landscape proactively. For instance, AI algorithms can analyze vast amounts of data from diverse sources, including network logs, intrusion detection systems, and user activities. By recognizing patterns associated with prior breaches, AI can flag anomalies that may signify an impending attack (Abed and Anupam, 2023). Such predictive capabilities allow organizations to allocate resources effectively and focus on high-risk areas, enhancing their overall security posture. Furthermore, continuous learning models can adapt to new threats by updating their predictive capabilities based on real-time data, ensuring that security measures evolve alongside the changing threat landscape.

Another critical aspect of predictive security models is the assessment of vulnerabilities within an organization's infrastructure. AI-based vulnerability assessment tools utilize machine learning to identify weaknesses in systems, applications, and networks that could be exploited by attackers. Traditional vulnerability scanning methods often rely on predefined databases and periodic assessments, which may not account for newly discovered vulnerabilities or specific environmental factors (Upadhyay and Sampalli, 2020). AI-enhanced vulnerability assessment tools can dynamically analyze an organization's systems and identify potential vulnerabilities in real time. These tools leverage data from threat intelligence feeds, system configurations, and historical attack data to prioritize vulnerabilities based on their potential impact. By focusing on high-risk vulnerabilities, organizations can implement targeted remediation efforts, thereby reducing their attack surface and enhancing their resilience to cyber threats. Additionally, AI can assist in identifying vulnerabilities that may not be immediately obvious through conventional assessment methods. For example, machine learning algorithms can analyze code repositories and application behaviors to detect security flaws that could lead to exploitation. By employing AI for vulnerability assessment, organizations can improve their overall security by addressing weaknesses before they are exploited.

AI plays a vital role in risk management by enabling organizations to develop proactive defense strategies. Traditional risk management approaches often involve assessing potential threats and their associated impacts on business operations. However, AI can enhance this process by providing real-time insights into evolving threats and vulnerabilities, allowing organizations to adapt their strategies accordingly as explain in figure 4 (Shah, 2021; Wan *et al.*, 2022).

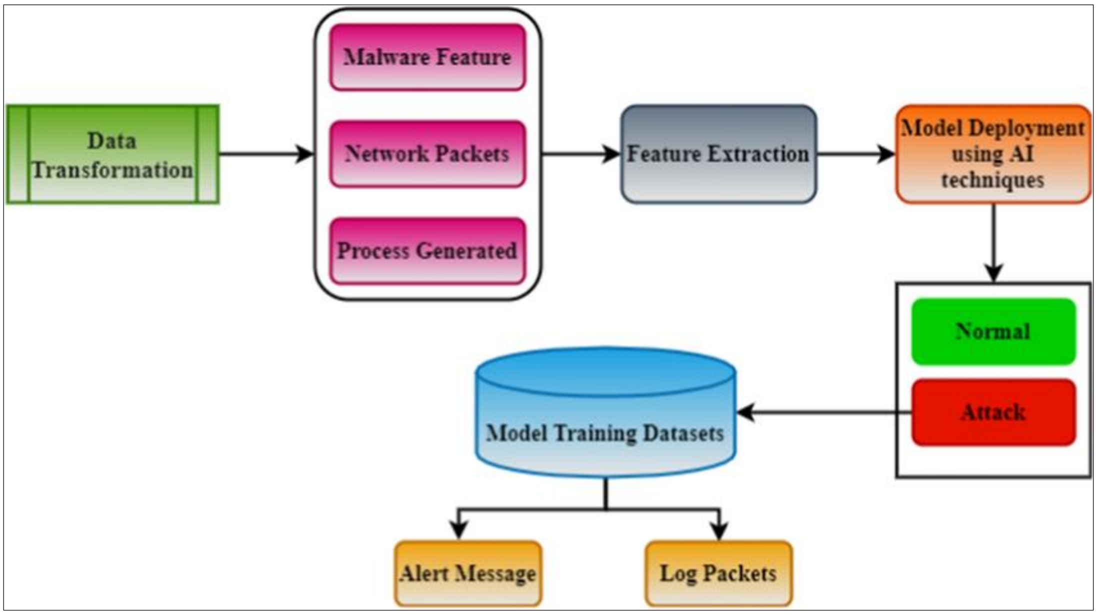

Figure 4 AI-powered forecasting of cyberattacks (Wan *et al.*, 2022)

AI-driven risk management tools can analyze data from various sources, including internal security logs, threat intelligence feeds, and external factors such as geopolitical events. By synthesizing this information, AI models can provide organizations with a comprehensive view of their risk landscape, enabling informed decision-making. For instance, AI can assist in determining the likelihood of specific attack vectors and the potential consequences of a breach, allowing organizations to prioritize their security investments effectively. Moreover, AI can facilitate the implementation of proactive defense strategies by automating threat detection and response processes. Automated systems can continuously monitor network traffic and user behavior, identifying anomalies that may indicate a security breach. By responding to threats in real time, organizations can mitigate potential damages and improve their overall security posture.

Several organizations have successfully implemented predictive AI models to enhance their cybersecurity efforts (Sen *et al.*, 2022). For instance, IBM's Watson for Cyber Security employs machine learning algorithms to analyze vast amounts of unstructured data, including blogs, reports, and forums, to identify potential threats and emerging attack patterns. By integrating this information with internal security data, Watson can provide security teams with actionable insights, enabling them to respond proactively to evolving threats. Another notable example is Darktrace, a cybersecurity firm that uses AI to detect and respond to cyber threats in real time. Their self-learning AI platform analyzes network traffic and user behavior to identify anomalies that may indicate a breach. Darktrace's technology has been employed across various sectors, demonstrating its effectiveness in adapting to unique environments and threat landscapes. By employing predictive models (Qumer and Ikrama, 2022), Darktrace has successfully thwarted numerous cyberattacks by providing organizations with early warnings and automated responses to potential threats. Additionally, Cisco's AI-driven security solutions utilize predictive analytics to enhance threat detection and response capabilities. Their platform aggregates data from multiple sources, applying machine learning algorithms to identify potential vulnerabilities and assess risks. By leveraging predictive AI, Cisco enables organizations to stay ahead of cyber threats and enhance their overall security frameworks.

The cybersecurity landscape has changed as a result of AI's integration with predictive security models, which allow enterprises to identify weaknesses, foresee threats, and take proactive measures to defend themselves. Organizations can more efficiently manage resources by using AI's predictive analytics to spot patterns that indicate possible assaults (Montasari *et al.*, 2021). AI-based vulnerability assessment tools make it easier to find vulnerabilities and make sure that areas that provide the greatest risk are fixed first. Furthermore, AI's contribution to risk management enables automated threat identification and reaction as well as well-informed decision-making. Case studies of organizations leveraging predictive AI models demonstrate the efficacy of these tools in enhancing cybersecurity efforts. As cyber threats continue to evolve, the importance of predictive AI in safeguarding digital assets will only grow, making it an essential component of modern cybersecurity frameworks.

2.4. Challenges of AI in Cybersecurity

The increasing integration of Artificial Intelligence (AI) into cybersecurity frameworks offers several advantages, including improved threat identification, automated incident response, and predictive analytics. To guarantee the ethical and successful application of AI in cybersecurity, there are important obstacles that come along with these benefits. The rise of hostile AI is one of the most urgent issues in the field of AI in cybersecurity (Egbuna, 2021). Cybercriminals are using artificial intelligence (AI) techniques more often to craft complex attacks that evade conventional security measures. Adversarial AI is the process of tricking machine learning algorithms with misleading inputs intended to yield inaccurate results. This approach can be employed in various ways, such as evading detection by intrusion detection systems or generating convincing phishing emails that bypass spam filters. For instance, attackers can use adversarial techniques to modify malware in such a way that it appears benign to AI-driven security systems. This tactic can undermine the effectiveness of AI in detecting and mitigating threats, creating a new arms race between cybersecurity professionals and malicious actors. As AI systems become more prevalent, the risk of adversarial attacks will likely increase, necessitating the development of robust defenses against such tactics (Aldahdooh *et al.*, 2022). Furthermore, AI-driven attacks can enable malicious actors to automate and scale their efforts, leading to a higher volume of attacks that may overwhelm existing security infrastructures. This challenge emphasizes the need for continuous improvement and adaptation of AI models to defend against evolving threats.

The deployment of AI in cybersecurity often involves the collection and analysis of vast amounts of data, raising significant data privacy concerns. AI systems require access to sensitive information to train models effectively, which may include personally identifiable information (PII), financial data, and other confidential data (Dash *et al.*, 2022). The aggregation of this data, combined with the potential for breaches or misuse, poses a substantial risk to individuals' privacy rights (Citron and Solove, 2022). Moreover, the use of AI algorithms can inadvertently lead to biased decision-making. For example, if an AI system is trained on biased datasets, it may disproportionately flag certain individuals or groups as potential threats based on flawed assumptions. This bias can have far-reaching consequences, including wrongful accusations or the exclusion of certain demographics from essential services. Addressing these privacy concerns requires implementing robust data protection measures, including anonymization, encryption, and strict data access controls (Thapa and Camtepe, 2021). Additionally, organizations must ensure compliance with privacy regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which mandate stringent guidelines for the collection and processing of personal data.

Trust and transparency in AI decision-making processes are critical components of successful AI integration into cybersecurity (Hamon *et al.*, 2022). Many organizations face challenges in explaining how AI models arrive at specific conclusions or recommendations, leading to skepticism among users and stakeholders. This lack of transparency can hinder the acceptance of AI technologies, as individuals may be reluctant to rely on systems that they do not fully understand. Furthermore, the "black box" nature of many AI algorithms, particularly deep learning models, complicates efforts to assess their reliability and efficacy (Tschider, 2020). Users may struggle to grasp how these models make decisions, resulting in a lack of trust in their outputs. This situation is especially concerning in cybersecurity, where decision-making can have significant consequences for organizational security. To build trust in AI-driven cybersecurity systems, organizations must prioritize transparency by providing clear explanations of how AI models operate and the factors influencing their decisions. Additionally, implementing explainable AI (XAI) techniques can help demystify AI processes, allowing stakeholders to understand and evaluate the reliability of AI outputs (Langer *et al*., 2021).

The ethical implications of AI in cybersecurity are another significant challenge. The deployment of AI technologies can raise ethical questions related to surveillance, consent, and the potential for abuse (Fontes *et al*., 2022). For example, organizations may use AI to monitor employee behavior or analyze user data for security purposes, leading to concerns about privacy invasion and the ethical use of surveillance technologies. Moreover, the regulatory landscape surrounding AI in cybersecurity remains evolving. Policymakers are grappling with how to regulate AI technologies effectively to mitigate potential harms while fostering innovation (Lescrauwaet *et al*., 2022). The lack of clear regulations can create uncertainty for organizations seeking to implement AI-driven solutions, as they may be unsure about compliance requirements or potential liabilities. To navigate these ethical and regulatory challenges, organizations must adopt a proactive approach by establishing clear ethical guidelines for AI use in cybersecurity. Engaging stakeholders, including ethicists, legal experts, and affected communities, can help ensure that AI applications align with societal values and promote responsible practices (Golbin *et al*., 2020).

AI's integration with cybersecurity offers potential as well as difficulties. Although AI has a great deal of promise to improve threat detection and response, it also comes with dangers pertaining to data protection, trust, ethics, and aggressive AI (Banik and Dandyala, 2023). A complex strategy that includes strong defenses against adversarial attacks, strict data protection measures, improved openness in AI decision-making, and unambiguous ethical principles is needed to address these difficulties. Through efficient navigation of these difficulties, businesses can leverage AI's capacity to strengthen cybersecurity operations while maintaining a focus on ethical and regulatory considerations.

2.5. AI’s Role in Security Compliance

Organizations are looking for effective strategies to manage compliance as the complexity of regulatory requirements for data security and privacy increases (Olukoya, 2022). In this sense, artificial intelligence (AI) has become a transformative tool, providing continuous monitoring and auditing capabilities, automating compliance processes, guaranteeing adherence to strict regulatory frameworks, and lowering compliance costs while increasing operational efficiency.

One of the most significant contributions of AI to security compliance is its ability to automate routine and repetitive compliance tasks. Traditional compliance processes often require manual checking and verification of security measures, which can be time-consuming and prone to human error (Fantoni *et al*., 2021). AI, however, offers automation solutions that can handle large volumes of data and complex rules with greater speed and precision. For instance, AI-powered systems can automatically scan databases and systems to ensure compliance with regulatory requirements. This includes validating encryption protocols, verifying data access controls, and monitoring data flows in real-time. Automated compliance tools allow organizations to not only maintain compliance with regulations but also to anticipate and address issues before they escalate into violations. By reducing the dependency on manual interventions, AI minimizes the risk of non-compliance and enhances the accuracy of the compliance processes.

AI plays a crucial role in ensuring that organizations adhere to various regulatory frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) (Silva and Soto, 2022). These regulations require organizations to maintain stringent control over how they handle personal data, implement privacy safeguards, and ensure transparency with individuals about how their data is used. AI systems can automatically analyze an organization’s data handling practices and ensure that they comply with the requirements set by these regulations. For example, AI can help monitor and control how personally identifiable information (PII) is accessed and processed within the organization, ensuring that data usage conforms to GDPR's principle of data minimization. Similarly, AI can enhance HIPAA compliance by ensuring that patient health information is encrypted and that only authorized personnel have access to sensitive data. Moreover, AI’s predictive analytics capabilities allow organizations to proactively identify potential regulatory risks and take steps to mitigate them (Ganesh and Kalpana, 2022). This helps in staying ahead of evolving compliance requirements and preventing breaches that could result in legal penalties.

AI’s ability to provide continuous monitoring and auditing is a game-changer for security compliance. Traditional compliance audits are periodic and retrospective, meaning that they only assess compliance at specific points in time, which can leave gaps between audits where violations may occur (Moon and Krahe, 2020). AI, on the other hand, enables continuous, real-time monitoring of compliance by constantly scanning systems for deviations from established regulatory guidelines. AI-powered compliance tools can continuously track and audit an organization's processes, detecting anomalies or suspicious activities that might indicate a potential breach of compliance. For example, AI can monitor access logs and identify unauthorized access attempts or unusual patterns of data movement, which may suggest a violation of compliance rules. This real-time insight allows organizations to respond to potential issues immediately, reducing the likelihood of regulatory breaches and ensuring sustained compliance. Additionally, AI can automate the generation of compliance reports, reducing the time and effort required for audits. This automated auditing process not only enhances transparency but also makes it easier for organizations to demonstrate compliance to regulatory authorities during formal inspections or inquiries (Bakhshi and Ghita, 2021).

The manual processes traditionally involved in maintaining compliance are often resource-intensive and costly. They require substantial investment in human resources, time, and technology. AI's automation capabilities significantly reduce these costs by streamlining compliance operations and eliminating the need for extensive manual interventions (Ng *et al.*, 2021). By leveraging AI, organizations can reduce the costs associated with compliance management in several ways. AI systems can automatically update themselves to remain in line with changing regulatory requirements, reducing the need for manual reconfiguration. Additionally, automated compliance tools reduce the risk of fines and penalties by helping organizations avoid compliance breaches, which could otherwise result in significant financial repercussions (Garrett and Mitchell, 2020). AI also improves operational efficiency by reducing the administrative burden on compliance teams. For example, AI-driven systems can manage the complexities of data privacy regulations more efficiently, enabling faster decision-making and more accurate assessments. This allows organizations to allocate their human resources to more strategic, value-added activities rather than getting bogged down in manual compliance tasks. AI has a transformative impact on security compliance by automating processes, ensuring adherence to regulatory frameworks, providing continuous monitoring, and reducing costs while improving efficiency. As regulatory landscapes continue to evolve, the integration of AI into compliance frameworks will become increasingly essential for organizations striving to meet their security and privacy obligations (Nguyen and Tran, 2023). Through its ability to enhance accuracy, efficiency, and real-time response, AI serves as a vital tool for managing the complexities of modern security compliance.

2.6. Enhancing Cybersecurity Governance with AI

Organizations confront never-before-seen difficulties in controlling risks, guaranteeing compliance, and upholding security procedures in the rapidly changing field of cybersecurity (Rawat, 2023). Artificial Intelligence (AI) emerges as a valuable ally in increasing cybersecurity governance by automating processes, giving insights, and improving overall efficiency. Enforcing security policies and procedures, monitoring and reporting compliance metrics, detecting fraud and facilitating regulatory reporting, and coordinating cybersecurity practices with compliance standards are the four key areas of AI's role in improving cybersecurity governance that are examined in this article.

AI plays a pivotal role in enforcing security policies and procedures within organizations. Traditional methods of policy enforcement often rely on manual processes, which can be inconsistent and error-prone (Mayr-Dorn *et al.*, 2021). AI-driven systems enable organizations to automate the enforcement of security policies by continuously monitoring user behavior, access controls, and network activities. For example, AI algorithms can analyze patterns of user activity to ensure compliance with established security protocols, automatically flagging any deviations or anomalies. Moreover, AI can facilitate the implementation of adaptive security measures that respond in real-time to emerging threats (Gudala *et al.*, 2021). By analyzing vast amounts of data and learning from past incidents, AI systems can enforce dynamic security policies that evolve to meet changing risk landscapes. This proactive approach enhances an organization's resilience against cyber threats and ensures that security measures are consistently applied across all levels of the organization.

In the realm of cybersecurity governance, tracking and reporting compliance metrics are essential for assessing an organization's adherence to regulatory requirements and internal security standards (Mantelero *et al.*, 2020). AI can streamline this process by automating the collection and analysis of compliance data. By integrating with various data sources, AI systems can aggregate information on security incidents, policy adherence, and risk assessments, providing real-time insights into an organization's compliance posture. AI's data analysis capabilities allow organizations to generate comprehensive compliance reports with minimal manual intervention (Falco *et al.*, 2021). This automation not only saves time and resources but also enhances the accuracy and reliability of compliance metrics. Additionally, AI can identify trends and patterns in compliance data, enabling organizations to make informed decisions and implement corrective actions when necessary.

Fraud detection is a critical component of cybersecurity governance, and AI has proven to be an invaluable tool in identifying and mitigating fraudulent activities. Machine learning algorithms can analyze vast datasets to detect unusual patterns or anomalies indicative of potential fraud (Bakumenko and Elragal, 2022). For instance, AI systems can monitor financial transactions, user behavior, and access logs in real time, flagging any suspicious activities for further investigation. Furthermore, AI aids in regulatory reporting by automating the process of generating required reports and ensuring that they meet compliance standards. Organizations must often report various metrics related to security incidents, fraud, and compliance activities to regulatory bodies. AI-driven systems can streamline this reporting process, ensuring that organizations maintain compliance while reducing the administrative burden associated with regulatory requirements. The integration of AI in fraud detection and regulatory reporting not only enhances security governance but also builds trust with stakeholders, as organizations demonstrate their commitment to maintaining robust security measures and adhering to regulatory standards.

Aligning cybersecurity practices with compliance standards is a critical challenge for organizations in today's regulatory environment (Marotta and Madnick, 2021). AI plays a significant role in ensuring that cybersecurity measures are consistent with various regulatory frameworks, such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and others. AI systems can analyze the specific requirements of these regulations and assess an organization's existing cybersecurity practices against these standards. By identifying gaps and vulnerabilities, AI provides actionable insights that enable organizations to align their cybersecurity strategies with compliance requirements (Kaur *et al.*, 2023). Moreover, AI can facilitate continuous compliance monitoring, ensuring that organizations remain compliant as regulations evolve. Through its ability to assess and adapt to changing regulatory landscapes, AI empowers organizations to proactively manage their cybersecurity governance (Judijanto *et al.*, 2022). This not only enhances compliance but also fosters a culture of security awareness and accountability throughout the organization.

By strengthening the enforcement of security policies, automating compliance tracking and reporting, enhancing fraud detection, and bringing practices into conformity with regulations, artificial intelligence is completely changing cybersecurity governance. Organizations must use AI technology to bolster their governance frameworks and guarantee strong security measures as cyber dangers continue to increase (Safitra *et al.*, 2023). Organizations can attain a proactive and adaptive approach to governance by incorporating AI into their cybersecurity plans. This will ultimately strengthen their resilience against cyber threats and ensure compliance in a complicated regulatory environment.

2.7. Future Trends and Developments in AI-Driven Cybersecurity

Artificial Intelligence (AI) integration into cybersecurity strategies is becoming more and more important as the digital world changes (Al-Mansoori and Salem, 2023). The field of AI-driven cybersecurity is expected to make considerable strides in the future due to the advent of new technologies and the increasing complexity of cyber threats. This examines four major trends and developments in cybersecurity: the influence of AI and quantum computing, the emergence of AI-based solutions designed for SME's, the possibility of AI-human cooperation in improving security, and the emergence of autonomous cybersecurity agents.

Quantum computing represents a paradigm shift in computational capabilities, promising unprecedented processing power that could revolutionize various fields, including cybersecurity. The synergy between AI and quantum computing has the potential to enhance cybersecurity measures significantly. Quantum computing can process vast amounts of data at incredible speeds, enabling the rapid analysis of security threats and vulnerabilities (Kumar *et al.*, 2022). However, this technological advancement also poses significant challenges. Quantum computers have the capability to break traditional encryption methods, which could render many existing security protocols obsolete. To counter this threat, researchers are exploring quantum-resistant cryptographic algorithms, and AI can play a vital role in developing these new security frameworks. By leveraging AI's analytical capabilities, organizations can create more robust encryption methods that are resistant to the potential threats posed by quantum computing, ensuring the continued protection of sensitive data (Lindsay, 2020; Girasa and Scalabrini, 2022).

Small and medium-sized enterprises (SMEs) have historically faced significant barriers in adopting advanced cybersecurity solutions due to limited resources and expertise. However, the rise of AI-driven cybersecurity solutions tailored specifically for SMEs is changing this landscape (Watney and Auer, 2021). These solutions offer scalable, cost-effective, and user-friendly security measures that empower SMEs to protect themselves against cyber threats. AI-based tools can automate routine security tasks, such as monitoring for threats, responding to incidents, and managing vulnerabilities. By harnessing AI, SMEs can enhance their cybersecurity posture without the need for extensive in-house expertise. Furthermore, the proliferation of cloud-based AI security solutions allows SMEs to access sophisticated tools and services that were previously only available to larger organizations. As the market for AI-driven cybersecurity solutions for SMEs continues to grow, it will enable these businesses to enhance their security measures and mitigate risks effectively (Manoharan and Sarker, 2023).

While AI offers powerful capabilities for automating and optimizing cybersecurity practices, the collaboration between AI systems and human expertise will be essential for maximizing security outcomes. The potential for AI-human collaboration lies in the complementary strengths of each. AI can process vast amounts of data, identify patterns, and detect anomalies at speeds beyond human capability, while human analysts possess contextual knowledge, intuition, and critical thinking skills (Mele *et al*., 2022). This collaboration can enhance threat detection and response efforts. For instance, AI can analyze network traffic to flag unusual behavior, while human experts can interpret the findings, investigate further, and make strategic decisions on how to respond. This synergy not only improves incident response times but also reduces the likelihood of false positives, enabling organizations to focus their resources on genuine threats. As organizations embrace this collaborative approach, the role of cybersecurity professionals will evolve, shifting towards a more strategic focus that leverages AI as a critical tool in their arsenal (Kjeldsen, 2022).

One of the most exciting developments in AI-driven cybersecurity is the emergence of autonomous cybersecurity agents (Jayakumar *et al*., 2021). These agents leverage machine learning and AI algorithms to independently monitor, detect, and respond to threats in real time without human intervention. Autonomous agents can analyze network behavior, identify vulnerabilities, and even execute pre-defined responses to mitigate threats automatically (Repetto *et al*., 2021). The deployment of these agents can significantly enhance an organization's security posture by providing rapid responses to evolving threats. For example, if an autonomous agent detects a potential breach, it can take immediate action by isolating affected systems, notifying relevant personnel, and implementing countermeasures to contain the threat. This level of responsiveness is crucial in an era where cyber threats are increasingly sophisticated and fast-moving. Moreover, autonomous cybersecurity agents can learn and adapt over time, continually improving their capabilities and effectiveness. As AI technologies evolve, the potential for these agents to operate in complex environments while coordinating with other security tools will redefine the cybersecurity landscape (Sobb *et al*., 2020).

Innovations and trends that will change the way businesses defend themselves against changing cyberthreats will define the future of AI-driven cybersecurity. The potential for AI-human collaboration, the introduction of autonomous cybersecurity agents, the integration of AI with quantum computing, and the rise of customized solutions for SMEs are all expected to improve cybersecurity governance (Gill *et al*., 2022; Nikolinakos, 2023). Organizations need to be proactive in implementing AI-driven solutions as these trends develop in order to stay ahead of dangers and guarantee strong security measures in a world that is becoming more and more digital. Accepting these technologies will be essential to preserving a strong cybersecurity posture in the face of escalating difficulties.

3. Conclusion

Artificial intelligence (AI) is improving threat detection, incident response, and regulatory adherence, which is radically changing the cybersecurity and security compliance landscape. The capacity to examine extensive datasets, recognize intricate attacks, and mechanize repetitive tasks considerably enhances an organization's defense against cyberattacks. Artificial intelligence (AI)-powered solutions enable companies, particularly small and medium-sized businesses (SMEs), by offering scalable solutions that improve their security posture and expedite compliance with regulatory frameworks such as GDPR and HIPAA.

But there are difficulties and moral dilemmas with integrating AI into cybersecurity. There are many obstacles to overcome, including hostile AI, data privacy, and the requirement for transparency in AI decision-making processes. In order to guarantee that AI systems are not only efficient but also implemented ethically and compliant with regulations, organizations need to manage these obstacles. Resolving these issues is essential to preserving the integrity of security procedures and fostering stakeholder trust.

In the future, AI has a promising role in bolstering security frameworks and compliance. AI will make it easier for businesses to create proactive, flexible security solutions that keep up with changing threat landscapes as technology advances. Innovative technologies like AI-powered predictive models and self-governing cybersecurity bots will make it easier for enterprises to foresee and reduce threats. Through promoting a cooperative strategy between AI systems and human knowledge, enterprises may build robust security frameworks that can address present issues as well as adjust to unforeseen circumstances in the future. In summary, AI has the ability to significantly transform cybersecurity and compliance, and a secure digital future will depend greatly on its ethical application and ongoing development.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclsoed.

References

[1] Abed, A.K. and Anupam, A., 2023. Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy*, *6*(3), p.e285.

[2] Aldahdooh, A., Hamidouche, W., Fezza, S.A. and Déforges, O., 2022. Adversarial example detection for DNN models: A review and experimental comparison. *Artificial Intelligence Review*, *55*(6), pp.4403-4462.

[3] Ali, S., Rehman, S.U., Imran, A., Adeem, G., Iqbal, Z. and Kim, K.I., 2022. Comparative evaluation of ai-based techniques for zero-day attacks detection. *Electronics*, *11*(23), p.3934.

[4] Alkatheiri, M.S., 2022. Artificial intelligence assisted improved human-computer interactions for computer systems. *Computers and Electrical Engineering*, *101*, p.107950.

[5] Al-Mansoori, S. and Salem, M.B., 2023. The role of artificial intelligence and machine learning in shaping the future of cybersecurity: trends, applications, and ethical considerations. *International Journal of Social Analytics*, *8*(9), pp.1-16.

[6] Anitha, C., Komala, C.R., Vivekanand, C.V., Lalitha, S.D. and Boopathi, S., 2023, February. Artificial Intelligence driven security model for Internet of Medical Things (IoMT). In *2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 1-7). IEEE.

[7] Aslam, M., Khan Abbasi, M.A., Khalid, T., Shan, R.U., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D.A. and Ahmad, R., 2022. Getting smarter about smart cities: Improving data security and privacy through compliance. *Sensors*, *22*(23), p.9338.

[8] Azzam, M., Pasquale, L., Provan, G. and Nuseibeh, B., 2021. Grounds for suspicion: Physics-based early warnings for stealthy attacks on industrial control systems. *IEEE Transactions on Dependable and Secure Computing*, *19*(6), pp.3955-3970.

[9] Bakhshi, T. and Ghita, B., 2021. Perspectives on Auditing and Regulatory Compliance in Blockchain Transactions. In *Trust Models for Next-Generation Blockchain Ecosystems* (pp. 37-65). Cham: Springer International Publishing.

[10] Bakumenko, A. and Elragal, A., 2022. Detecting anomalies in financial data using machine learning algorithms. *Systems*, *10*(5), p.130.

[11] Banik, S. and Dandyala, S.S.M., 2023. The Role of Artificial Intelligence in Cybersecurity Opportunities and Threats. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(04), pp.420-440.

[12] Bécue, A., Praça, I. and Gama, J., 2021. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), pp.3849-3886.

[13] Bonfanti, M.E., 2022. Artificial intelligence and the offence-defence balance in cyber security. *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation. London: Routledge*, pp.64-79.

[14] Calvo, M. and Beltrán, M., 2022. A model for risk-based adaptive security controls. *Computers & Security*, *115*, p.102612.

[15] Challa, N., 2022. Unveiling the Shadows: A Comprehensive Exploration of Advanced Persistent Threats (APTs) and Silent Intrusions in Cybersecurity. *Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-204. DOI: doi. org/10.47363/JAICC/2022 (1)*, *190*, pp.2-5.

[16] Chouraik, C., El Founir, R. And Taibi, K., 2024. The Impact of AI on Cybersecurity: A New Paradigm for Threat Management. *African Journal of Management, Engineering and Technology*, *2*(2), pp.92-100.

[17] Citron, D.K. and Solove, D.J., 2022. Privacy harms. *BUL Rev.*, *102*, p.793.

[18] Dasgupta, D., Akhtar, Z. and Sen, S., 2022. Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), pp.57-106.

[19] Dash, B., Sharma, P. and Ali, A., 2022. Federated learning for privacy-preserving: A review of PII data analysis in Fintech. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(4).

[20] Egbuna, O.P., 2021. The Impact of AI on Cybersecurity: Emerging Threats and Solutions. *Journal of Science & Technology*, *2*(2), pp.43-67.

[21] Falco, G., Shneiderman, B., Badger, J., Carrier, R., Dahbura, A., Danks, D., Eling, M., Goodloe, A., Gupta, J., Hart, C. and Jirotka, M., 2021. Governing AI safety through independent audits. *Nature Machine Intelligence*, *3*(7), pp.566-571.

[22] Fantoni, G., Al-Zubaidi, S.Q., Coli, E. and Mazzei, D., 2021. Automating the process of method-time-measurement. *International Journal of Productivity and Performance Management*, *70*(4), pp.958-982.

[23] Fontes, C., Hohma, E., Corrigan, C.C. and Lütge, C., 2022. AI-powered public surveillance systems: why we (might) need them and how we want them. *Technology in Society*, *71*, p.102137.

[24] Foorthuis, R., 2021. On the nature and types of anomalies: a review of deviations in data. *International journal of data science and analytics*, *12*(4), pp.297-331.

[25] Ganesh, A.D. and Kalpana, P., 2022. Future of artificial intelligence and its influence on supply chain risk management–A systematic review. *Computers & Industrial Engineering*, *169*, p.108206.

[26] Gao, R., Zhang, Z., Shi, Z., Xu, D., Zhang, W. and Zhu, D., 2021, October. A review of natural language processing for financial technology. In *International Symposium on Artificial Intelligence and Robotics 2021* (Vol. 11884, pp. 262-277). SPIE.

[27] Garrett, B.L. and Mitchell, G., 2020. Testing compliance. *Law & Contemp. Probs.*, *83*, p.47.

[28] Gill, S.S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A. and Singh, M., 2022. AI for next generation computing: Emerging trends and future directions. *Internet of Things*, *19*, p.100514.

[29] Girasa, R. and Scalabrini, G.J., 2022. Regulation of innovative technologies: blockchain, artificial intelligence and quantum computing. Springer Nature.

[30] Golbin, I., Rao, A.S., Hadjarian, A. and Krittman, D., 2020, December. Responsible AI: a primer for the legal community. In *2020 IEEE international conference on big data (big data)* (pp. 2121-2126). IEEE.

[31] Gudala, L., Shaik, M. and Venkataramanan, S., 2021. Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies. *Journal of Artificial Intelligence Research*, *1*(2), pp.19-45.

[32] Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L. and Pospelova, V., 2022. The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence*, *36*(1), p.2037254.

[33] Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G. and De Hert, P., 2022. Bridging the gap between AI and explainability in the GDPR: towards trustworthiness-by-design in automated decision-making. *IEEE Computational Intelligence Magazine*, *17*(1), pp.72-85.

[34] Hejase, H.J., Fayyad-Kazan, H.F. and Moukadem, I., 2020. Advanced persistent threats (apt): An awareness review. *Journal of Economics and Economic Education Research*, *21*(6), pp.1-8.

[35] Hina, S. and Dominic, P.D.D., 2020. Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*.

[36] Jayakumar, P., Brohi, S.N. and Jhanjhi, N.Z., 2021. Artificial intelligence and military applications: Innovations, cybersecurity challenges & open research areas.

[37] Jimmy, F., 2021. Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, pp.564-574.

[38] Judijanto, L., Asfahani, A., Bakri, A.A., Susanto, E. and Kulsum, U., 2022. AI-Supported Management through Leveraging Artificial Intelligence for Effective Decision Making. *Journal of Artificial Intelligence and Development*, *1*(1), pp.59-68.

[39] Kaloudi, N. and Li, J., 2020. The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), pp.1-34.

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

[41] Kjeldsen, O., 2022. Modern & Resilient Cybersecurity The Need for Principles, Collaboration, Innovation, Education & the Occasional Application of Power. In *Cybersecurity and Privacy-Bridging the Gap* (pp. 135-160). River Publishers.

[42] Kumar, A., Bhushan, B., Shriti, S. and Nand, P., 2022. Quantum computing for health care: a review on implementation trends and recent advances. *Multimedia Technologies in the Internet of Things Environment, Volume 3*, pp.23-40.

[43] Kuzlu, M., Fair, C. and Guler, O., 2021. Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things*, *1*(1), p.7.

[44] Langer, M., Oster, D., Speith, T., Hermanns, H., Kästner, L., Schmidt, E., Sesing, A. and Baum, K., 2021. What do we want from Explainable Artificial Intelligence (XAI)?–A stakeholder perspective on XAI and a conceptual model guiding interdisciplinary XAI research. *Artificial Intelligence*, *296*, p.103473.

[45] Lescrauwaet, L., Wagner, H., Yoon, C. and Shukla, S., 2022. Adaptive legal frameworks and economic dynamics in emerging tech-nologies: Navigating the intersection for responsible innovation. *Law and Economics*, *16*(3), pp.202-220.

[46] Lindsay, J.R., 2020. Demystifying the quantum threat: infrastructure, institutions, and intelligence advantage. *Security Studies*, *29*(2), pp.335-361.

[47] Maddireddy, B.R. and Maddireddy, B.R., 2021. Evolutionary Algorithms in AI-Driven Cybersecurity Solutions for Adaptive Threat Mitigation. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), pp.17-43.

[48] Madhuri, T.S., Babu, E.R., Uma, B. and Lakshmi, B.M., 2023. Big-data driven approaches in materials science for real-time detection and prevention of fraud. *Materials Today: Proceedings*, *81*, pp.969-976.

[49] Manoharan, A. and Sarker, M., 2023. Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *DOI: https://www. doi. org/10.56726/IRJMETS32644*, *1*.

[50] Mantelero, A., Vaciago, G., Samantha Esposito, M. and Monte, N., 2020. The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, *28*(4), pp.297-328.

[51] Marotta, A. and Madnick, S., 2021. Convergence and divergence of regulatory compliance and cybersecurity. *Issues in Information Systems*, *22*(1).

[52] Mayr-Dorn, C., Vierhauser, M., Bichler, S., Keplinger, F., Cleland-Huang, J., Egyed, A. and Mehofer, T., 2021, May. Supporting quality assurance with automated process-centric quality constraints checking. In *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)* (pp. 1298-1310). IEEE.

[53] Mele, C., Marzullo, M., Morande, S. and Spena, T.R., 2022. How Artificial Intelligence enhances human learning abilities: opportunities in the fight against Covid-19. *Service Science*, *14*(2), pp.77-89.

[54] Mohamed, N., Alam, E. and Stubbs, G.L., 2022. Multi-layer protection approach MLPA for the detection of advanced persistent threat. *Journal of Positive School Psychology*, pp.4496-4518.

[55] Montasari, R., Carroll, F., Macdonald, S., Jahankhani, H., Hosseinian-Far, A. and Daneshkhah, A., 2021. Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. *Digital forensic investigation of internet of things (IoT) devices*, pp.47-64.

[56] Moon, D. and Krahel, J.P., 2020. Continuous risk monitoring and assessment: New component of continuous assurance. *Journal of Emerging Technologies in Accounting*, *17*(2), pp.173-200.

[57] Narsimha, B., Raghavendran, C.V., Rajyalakshmi, P., Reddy, G.K., Bhargavi, M. and Naresh, P., 2022. Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application. *IJEER*, *10*(2), pp.87-92.

[58] Nassar, A. and Kamal, M., 2021. Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management*, *5*(1), pp.51-63.

[59] Ng, K.K., Chen, C.H., Lee, C.K., Jiao, J.R. and Yang, Z.X., 2021. A systematic literature review on intelligent automation: Aligning concepts from theory, practice, and future perspectives. *Advanced Engineering Informatics*, *47*, p.101246.

[60] Nguyen, M.T. and Tran, M.Q., 2023. Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *International Journal of Intelligent Automation and Computing*, *6*(5), pp.1-12.

[61] Nikolinakos, N.T., 2023. Launching a European Initiative on Artificial Intelligence. In *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies-The AI Act* (pp. 23-98). Cham: Springer International Publishing.

[62] Olukoya, O., 2022. Assessing frameworks for eliciting privacy & security requirements from laws and regulations. *Computers & Security*, *117*, p.102697.

[63] Pang, G., Shen, C., Cao, L. and Hengel, A.V.D., 2021. Deep learning for anomaly detection: A review. *ACM computing surveys (CSUR)*, *54*(2), pp.1-38.

[64] Pham, Q.V., Nguyen, D.C., Huynh-The, T., Hwang, W.J. and Pathirana, P.N., 2020. Artificial intelligence (AI) and big data for coronavirus (COVID-19) pandemic: a survey on the state-of-the-arts. *IEEE access*, *8*, pp.130820-130839.

[65] Pulyala, S.R., Jangampet, V.D. and Desetty, A.G., 2023. REVOLUTIONIZING SIEM WITH ML-DRIVEN RISK ASSESSMENT AND PRIORITIZATION. *International Journal of Information Technology (IJIT)*, *4*(2), pp.55-62.

[66] Qumer, S.M. and Ikrama, S., 2022. Poppy Gustafsson: redefining cybersecurity through AI. *The Case for Women*, pp.1-38.

[67] Rangaraju, S., 2023. Secure by intelligence: enhancing products with AI-driven security measures. *EPH-International Journal of Science And Engineering*, *9*(3), pp.36-41.

[68] Rawat, S., 2023. Navigating the Cybersecurity Landscape: Current Trends and Emerging Threats. *Journal of Advanced Research in Library and Information Science*, *10*(3), pp.13-19.

[69] Reddy, A.R.P., 2021. The Role of Artificial Intelligence in Proactive Cyber Threat Detection In Cloud Environments. *NeuroQuantology*, *19*(12), pp.764-773.

[70] Repetto, M., Striccoli, D., Piro, G., Carrega, A., Boggia, G. and Bolla, R., 2021. An autonomous cybersecurity framework for next-generation digital service chains. *Journal of Network and Systems Management*, *29*(4), p.37.

[71] Safitra, M.F., Lubis, M. and Fakhrurroja, H., 2023. Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), p.13369.

[72] Schlette, D., Caselli, M. and Pernul, G., 2021. A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), pp.2525-2556.

[73] Sen, R., Heim, G. and Zhu, Q., 2022. Artificial intelligence and machine learning in cybersecurity: Applications, challenges, and opportunities for mis academics. *Communications of the Association for Information Systems*, *51*(1), p.28.

[74] Shah, V., 2021. Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Espanola de Documentacion Cientifica*, *15*(4), pp.42-66.

[75] Shukla, A.K., 2022. An efficient hybrid evolutionary approach for identification of zero-day attacks on wired/wireless network system. *Wireless Personal Communications*, *123*(1), pp.1-29.

[76] Silva, I. and Soto, M., 2022. Privacy-preserving data sharing in healthcare: an in-depth analysis of big data solutions and regulatory compliance. *International Journal of Applied Health Care Analytics*, *7*(1), pp.14-23.

[77] Sobb, T., Turnbull, B. and Moustafa, N., 2020. Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11), p.1864.

[78] Syed, F.M. and ES, F.K., 2022. Automating SOX Compliance with AI in Pharmaceutical Companies. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *13*(1), pp.383-412.

[79] Tao, F., Akhtar, M.S. and Jiayuan, Z., 2021. The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, *8*(28), pp.e3-e3.

[80] Tatineni, S. and Mustyala, A., 2022. Advanced AI Techniques for Real-Time Anomaly Detection and Incident Response in DevOps Environments: Ensuring Robust Security and Compliance. *Journal of Computational Intelligence and Robotics*, *2*(1), pp.88-121.

[81] Tayyab, U.E.H., Khan, F.B., Durad, M.H., Khan, A. and Lee, Y.S., 2022. A survey of the recent trends in deep learning based malware detection. *Journal of Cybersecurity and Privacy*, *2*(4), pp.800-829.

[82] Thapa, C. and Camtepe, S., 2021. Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, *129*, p.104130.

[83] Tschider, C.A., 2020. Beyond the" Black Box". *Denv. L. Rev.*, *98*, p.683.

[84] Upadhyay, D. and Sampalli, S., 2020. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, p.101666.

[85] Wan, B., Xu, C., Mahapatra, R.P. and Selvaraj, P., 2022. Understanding the cyber-physical system in international stadiums for security in the network from cyber-attacks and adversaries using AI. *Wireless Personal Communications*, *127*(2), pp.1207-1224.

[86] Watney, C.A.L.E.B. and Auer, D.I.R.K., 2021. Encouraging AI adoption by EU SMEs. *Progressive Policy Institute*.

[87] Whyte, C., 2020, May. Problems of Poison: New Paradigms and" Agreed" Competition in the Era of AI-Enabled Cyber Operations. In *2020 12th International Conference on Cyber Conflict (CyCon)* (Vol. 1300, pp. 215-232). IEEE.

[88] Yaseen, A., 2022. ACCELERATING THE SOC: ACHIEVE GREATER EFFICIENCY WITH AI-DRIVEN AUTOMATION. *International Journal of Responsible Artificial Intelligence*, *12*(1), pp.1-19.

[89] Zaman, S., Alhazmi, K., Aseeri, M.A., Ahmed, M.R., Khan, R.T., Kaiser, M.S. and Mahmud, M., 2021. Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, *9*, pp.94668-94690.

[90] Zeadally, S., Adi, E., Baig, Z. and Khan, I.A., 2020. Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access*, *8*, pp.23817-23837.

[91] Zibak, A., Sauerwein, C. and Simpson, A.C., 2022. Threat intelligence quality dimensions for research and practice. *Digital Threats: Research and Practice*, *3*(4), pp.1-22.