Global Journal on Innovation, Opportunities and Challenges in AAI and Machine Learning
http://eurekajournals.com/IJIOCAAIML.html
ISSN: 2581-5156

The Impact of Artificial Intelligence on Cybersecurity: Opportunities and Threats

Stephen-Nicolas Thompson[1], Jeffery Reid[1], Garson Hutchinson[1], Brian Davis[1], Clifton Foster[2], Dennis Brooks[3], Paul Andrew Bourne[1], PhD.

[1]Vocational Training Development Institute (VTDI), Kingston, Jamaica, WI.
[2]Northern Caribbean University, Manchester, Jamaica, WI.
[3]Jamaica Constabulary Force, Kingston, Jamaica, WI.

Abstract

Introduction: This study delves into the profound impact of Artificial Intelligence (AI) on cybersecurity. It specifically focuses on the comprehensive evaluation of AI's opportunities and threats, including enhanced threat detection, automated responses, the evolving nature of cyberattacks, and the challenges posed by AI-driven malicious activities.

Objectives: This research explores both the benefits and risks that Artificial Intelligence (AI) presents to cybersecurity. The primary focus is on quantifying and analysing the opportunities AI provides in improving security measures, such as real-time threat detection and predictive analytics, as well as the threats it introduces, including AI-powered cyberattacks and the weaponisation of AI The study offers comprehensive insights into the evolving landscape of cybersecurity in the AI era. It aims to provide valuable input for policy recommendations and augment understanding of the broader implications of AI in cybersecurity.

Methods and Materials: This quantitative study uses a structured questionnaire to investigate the impact of AI on cybersecurity among professionals in the field. Developed with 27 questions, the survey gathered primary data from 303 participants through snowball and convenience sampling. It includes closed-ended questions, employing a 5-point Likert scale for the final eight questions, and open-ended questions focusing on demographics, AI adoption, and cybersecurity challenges. Data collection was facilitated via Google Forms for accessibility, with analysis employing correlational techniques to explore relationships among variables such as the effectiveness of AI in threat detection, the occurrence of AI-driven cyberattacks, and other cybersecurity impacts, shedding light on the complex role of AI in modern cybersecurity practices.

Findings: The study reveals significant effects of AI on cybersecurity, highlighting both opportunities and threats. On average, respondents noted a 45% increase in threat detection efficiency due to AI implementations. However, 32% of participants reported encountering AI-driven cyberattacks, underscoring the dual-edged nature of AI in this field. The study also found that AI adoption led to a 40% reduction in response times to incidents, but it also revealed a 28% increase in sophisticated, AI-powered phishing attacks. These findings underscore the critical need to balance the advantages of AI with the emerging risks it presents in cybersecurity.

Conclusion: Artificial Intelligence (AI) significantly influences cybersecurity, presenting remarkable opportunities and serious threats. Recognising these impacts is crucial for shaping policies that leverage AIto enhance security while mitigating risks. This recognition necessitates the development of a comprehensive strategy that includes public education on AI's role in cybersecurity. Such education is vital for enhancing understanding and preparedness alongside evidence-based guidelines to manage the dual-edged nature of AI technologies. The urgency of this need cannot be overstated. Improving the development of AI governance frameworks is also vital for minimising risks and maximising the benefits of AI in cybersecurity. By integrating these measures, the cybersecurity industry can foster a safer digital environment and strengthen resilience against the growing threats posed by AI

Keywords: Artificial Intelligence, Cybersecurity, Threat Detection, AI-Powered Cyberattacks, Predictive Analytics, Cybersecurity Policy.

Introduction

Cybersecurity has become an increasingly critical concern in the digital age, with artificial intelligence (AI) expanding to protect and threaten digital infrastructure (Kaur et al., 2023). The Global Risk Report 2020 (World Economic Forum, 2020) recognised AI as a pivotal technology that will shape the future of cybersecurity, emphasising its potential to transform defensive and offensive cyber operations. Globally, there has been a noticeable increase in AI-driven cyberattacks, with statistics indicating that over 30% of cyberattacks in 2023 involved some form of AI or machine learning (Check Point Team, 2024).

According to Steele (2024), AIcanrevolutionise cybersecurity by enabling more effective threat detection and response. Using meta-analysis, Kaur et al. (2023) reviewed 2.395 studies, with 295 being primary ones, indicating, "The review also identifies future research opportunities in emerging cybersecurity application areas, advanced AI methods, data representation, and the development of new infrastructures for the successful adoption of AI-based cybersecurity in today's era of digital transformation and polycrisis." (p. 1). Notwithstanding the perspective of Kaur et al. (2023), if leveraged for malicious purposes, AI poses significant risks, potentially ushering in a new era of sophisticated cyberattacks; this threat is referred to as the weaponisation of AI (Giannaros et al., 2023; Hong et al. Team, 2024;Malatji&Tolah, 2024).

AI's rise in cybersecurity has profound implications for digital infrastructure security and the broader socio-economic landscape (Binhammad et al., 2024; De Azambuja et al., 2023; Kaur et al., 2023). AI technologies, including machine learning, natural language processing, and deep learning, are increasingly integrated into cybersecurity frameworks. (Binhammad et al., 2024; Roshanaei et al.,2024). (Binhammad et al., 2024; Roshanaei et al., 2024). These technologies enhance the ability to detect anomalies, predict potential threats, and respond rapidly to incidents. In industries such as finance, healthcare, and critical infrastructure, where data breaches and system disruptions can have catastrophic consequences, the integration of AI is particularly crucial. The ability to swiftly and accurately identify threats in these sectors protects sensitive data and safeguards essential services that society relies on. However, as AIbecomes more embedded in cybersecurity systems, it also opens up new avenues for exploitation by cybercriminals. AIcan be weaponised to create highly sophisticated and adaptive malware, automate phishing attacks, and conduct large-scale cyber espionage. The dual-use nature of AI in cybersecurity underscores the necessity for robust strategies to mitigate these emerging threats. The adaptability of AI-driven attacks means that traditional cybersecurity measures may become less effective, requiring continuously evolving defensive strategies to counteract increasingly complex threats. The potential for AI to be used as a tool for both protection and harm highlights the urgent need for a balanced approach in its deployment within cybersecurity frameworks and the need for adaptability in our defensive strategies.

In addition to AI's technical challenges in cybersecurity, significant ethical and regulatory concerns must be addressed. The increasing reliance on AI for cybersecurity raises questions about the accountability of AI systems, mainly when automated decision-making processes are involved (Jada &Mayayise, 2024; Osasona et al., 2024). There is also the potential for biased decision-making in automated threat assessments, which could result in unfair or disproportionate security measures. The ethical implications of AI in cybersecurity extend to issues such as data privacy, the transparency of AI algorithms, and the potential for AI-driven surveillance. As AIplays a more prominent role in cybersecurity, comprehensive research and policy development are needed to ensure that these powerful tools are used to protect, rather than undermine, the digital world. This involves not only technical solutions but also the establishment of ethical guidelines and regulatory frameworks that address the unique challenges posed by AI in cybersecurity because of the cost associated with the weaponisation of digital transformation (see Table 1).

The table provides a detailed overview of the increasing impact of AI-driven cyberattacks over the decade from 2014 to 2024. It presents four critical metrics for each year:

Table 1:

Year	Number of AI-driven cyberattacks	Percentage of Total Cyber attacks Involving AI	Average Financial Loss per Incident (USD)	Average Response Time to AI-Driven Attacks (Hours)
2014	120	5%	$150,000	24
2015	140	6%	$175,000	22
2016	180	7%	$200,000	20
2017	220	8%	$225,000	18
2018	300	10%	$250,000	16
2019	450	15%	$300,000	14
2020	600	20%	$350,000	12
2021	750	25%	$400,000	10
2022	900	30%	$450,000	8

2023	1,200	35%	$500,000	6
2024*	1,500	40%	$550,000	4

* As of August 23, 2024

Background of the Study

The rapid advancement of Artificial Intelligence (AI) has revolutionised various sectors, including cybersecurity (Jada &Mayayise, 2024).AI's ability to process vast amounts of data, recognise patterns, and predict potential threats has made it an invaluable tool in protecting digital infrastructure. However, the same capabilities that make AI a powerful defence mechanism also pose significant risks when exploited for malicious purposes. Over the past decade, there has been a marked increase in AI-driven cyberattacks, where threat actors utilise AI to develop more sophisticated and adaptive attack methods, such as automated phishing, deepfake technologies, and AI-powered malware. These attacks are more challenging to detect and faster and more efficient in breaching security measures, leading to more significant financial and operational losses for organisations worldwide.

The growing prevalence of AI in cybersecurity has prompted extensive research into its benefits and the emerging threats it poses. While AI enhances the ability of security systems to detect and respond to threats in real time, it also introduces new vulnerabilities that traditional security measures are ill-equipped to handle. The dual-edged nature of AI in cybersecurity necessitates a deeper understanding of how these technologies are being used, defensively and offensively. This study aims to explore the evolving landscape of cybersecurity in the AI era, focusing on the opportunities AI presents for improving security and the threats it introduces as cybercriminals increasingly harness AI for their purposes. By analysing these dynamics, the study seeks to provide insights to inform the development of more effective cybersecurity strategies and policies.

Statement of the Problem

As Artificial Intelligence (AI) continues to advance and integrate into various sectors, its impact on cybersecurity has become increasingly significant. While AI offers enhanced capabilities in detecting and mitigating cyber threats, it also introduces new vulnerabilities that malicious actors can exploit. The dual-edged nature of AI in cybersecurity presents a complex challenge: on the one hand, AI can dramatically improve the efficiency and effectiveness of security measures; on the other hand, it can also empower cybercriminals to execute more sophisticated and harder-to-detect attacks. As a result, the ongoing development of AI in cybersecurity requires a balanced approach, emphasising both innovation in defence mechanisms and vigilance against the potential misuse of AI by adversaries.

The research problem, therefore, revolves around understanding the full scope of AI's impact on cybersecurity, particularly in identifying and balancing the opportunities it provides with the emerging threats it creates. This study investigates how organisations leverage AI to enhance their cybersecurity frameworks while examining the potential risks and challenges that AI poses when used maliciously. The goal is to provide a comprehensive analysis of how AI is reshaping the cybersecurity landscape, focusing on both the benefits and the dangers, to inform the development of strategies that can effectively address these challenges. Ultimately, this research aims to contribute to creating robust, AI-driven cybersecurity solutions that capitalise on AI's strengths and proactively mitigate its associated risks.

Significance of the Study

This study's significance lies in its potential to provide valuable insights into the rapidly evolving field of cybersecurity, particularly in the context of Artificial Intelligence (AI). As AI technologies increasingly permeate cybersecurity systems, they are utilised to enhance threat detection, automate responses, and bolster overall security posture. This study examines the critical need to understand AI's impact on cybersecurity, a necessity driven by several key factors.

One of the primary contributions of this research is its potential to enhance cybersecurity practices by demonstrating how AIcan be effectively leveraged to improve threat detection and response mechanisms. By analysing the capabilities of AI in these areas, the study offers practical guidance for cybersecurity professionals. Such insights are invaluable for organisations seeking to strengthen their defences against the growing complexity and sophistication of cyber threats. In addition, the study delves into the risks associated with AI, specifically how cybercriminals can exploit it to conduct more advanced and difficult-to-detect attacks. Understanding these emerging threats is essential for developing proactive strategies to mitigate potential risks and protect sensitive information.

Furthermore, the research holds significant implications for policy and regulation. It provides critical insights that can assist policymakers and regulatory bodies in grasping the broader implications of AI in cybersecurity. This understanding is vital for crafting policies and regulations that balance harnessing AI's benefits and safeguarding against its potential misuse. Additionally, by exploring the dual-edged nature of AI in cybersecurity, the study lays the groundwork for future research in this area. It highlights key areas that require further investigation, encouraging the development of more comprehensive strategies to address the challenges and opportunities presented by AIFinally, the study offers valuable guidance to organisations by clarifying the opportunities and risks associated with AI in cybersecurity. This knowledge supports informed decision-making regarding technology adoption, risk management, and investment in AI-driven security solutions.

Purpose of the Study

On the positive side, AI has shown significant potential in enhancing cybersecurity measures through various applications. These include improving threat detection accuracy by analysing vast amounts of data at unprecedented speeds, reducing response times through automated threat response systems, and increasing the overall effectiveness of security protocols by continuously learning and adapting to new threats. The study highlights how AI-driven solutions can fortify cybersecurity infrastructures by identifying and evaluating these benefits, making them more resilient against an ever-evolving threat landscape.

Conversely, the study delves into the risks and challenges ofintegratingAI into cybersecurity. It will examine how cybercriminals increasingly leverageAI to develop more sophisticated and hard-to-detect attacks, such as AI-generated phishing schemes and automated malware. Additionally, the research will assess the current state of AI adoption in cybersecurity across various organisations and sectors, exploring the extent of AI integration into security operations and evaluating the effectiveness of these implementations. By providing insights and recommendations for policymakers, cybersecurity professionals, and organisations, this study aims to guide the development of robust strategies, policies, and regulations that maximise the benefits of AI while mitigating its potential risks. Ultimately, it seeks to contribute to the growing body of knowledge on AI in cybersecurity, offering a balanced understanding of its role as both a powerful defensive tool and a potential weapon for attackers.

Rationale of Study

According to Pierazzi et al. (2020), recent reviews of AI applications in cybersecurity highlight a critical gap in the literature, particularly concerning the potential vulnerabilities introduced by AI-driven systems. Their findings reveal that while there is extensive research on the technical advancements AI brings to cybersecurity, there is a noticeable lack of comprehensive studies addressing the associated risks, such as adversarial attacks and ethical concerns. This gap underscores the need for more balanced research in this rapidly evolving field. Consequently, this dissertation seeks to explore the dual-edged impact of AI on cybersecurity by examining its opportunities and risks.

General Research Question

Does integrating Artificial Intelligence in cybersecurity influence security measures and introduce new risks, particularly concerning adversarial attacks and ethical implications?

Specific Research Questions

This study aims to address the following key research questions:

1. What are the primary opportunities that AI provides in cybersecurity?
2. How extensively are organisations adopting AI for cybersecurity purposes, and what factors influence its implementation?
3. What future trends can be anticipated in AI and cybersecurity?

Definition of Terms

Artificial intelligence (AI) is a technology that enables computers and machines to simulate human learning, comprehension, problem-solving, decision-making, creativity, and autonomy.

Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyberattacks.

Threat detection is a defensive strategy that analyses a system's behaviour to identify potential security risks before they can cause damage.

An AI-powered threat attack is a cyberattack that uses artificial intelligence (AI) or machine learning (ML) to automate, enhance, or accelerate various phases of an attack.

Machine learning (ML) is a branch of artificial intelligence (AI) and computer science that focuses on using data and algorithms to enable AI to imitate how humans learn, gradually improving its accuracy.

Predictive analytics uses statistics and modelling techniques to determine future performance based on current and historical data.

A cybersecurity policy is a set of guidelines and procedures that an organisation uses to protect its digital assets from cyber threats.

CybercriI is a criminal activity that targets or uses a computer, a computer network or a networked device.

AI-driven solutions use artificial intelligence (AI) to automate tasks, analyse data, and make predictions.

Delimitations of the Study

1. **Complexity of AI Algorithms**: The study may not delve deeply into the technical intricacies of AI algorithms, particularly regarding how these algorithms function at a detailed level. This could limit understanding of the specific mechanisms through which AI influences cybersecurity, especially for non-technical audiences.
2. **Focus on Current Trends**: The study addresses contemporary developments in AI and cybersecurity, which may restrict its exploration of long-term implications. While providing valuable insights into current trends, the research may not fully anticipate future challenges or opportunities as AI technologies evolve.

Limitations of the Study

1. **Bias in Self-Reported Data**: The study's reliance on self-reported data from organisations or cybersecurity professionals introduces the potential for biases. Respondents may overestimate the effectiveness of AI in their security measures or under-report incidents involving AI-driven cyber threats, leading to a skewed representation of AI's impact on cybersecurity.

Review of Literature

Introduction

The literature review is structured around the following themes: 1. AI in cybersecurity, 2. opportunities presented by AI in enhancing cybersecurity, 3. threats and challenges posed by AI in the context of cybersecurity, 4. ethical and regulatory considerations, and 5. future directions for research in AI and cybersecurity. The section concludes by justifying the need for this study, emphasising the importance of understanding both the beneficial and detrimental effects of AI in cybersecurity.

Theoretical Framework

A theoretical framework provides assumptions and essential issues grounded in the study. This study uses a hybrid theoretical perspective, which constitutes more than two critical theories. Socio-technical systems theory, dual-use technology theory, technological determinism, and e**thical and regulatory theories** arewell-suited for understanding the role of AI in cybersecurity.

Socio-Technical Systems Theory suggests that technology, human actors, and social systems interact complexly to shape outcomes in technological domains such as cybersecurity. In this context, AI operates as a technical tool and as part of a broader system that includes organisational processes, human decision-making, and ethical considerations. AI enhances cybersecurity through automation and advanced threat detection, but the human dimension (such as malicious actors exploiting AI or implementing biased algorithms) adds complexity to its role. The socio-technical framework emphasises the importance of considering how AI interacts with human and organisational factors, underscoring the need for cybersecurity policies and governance that address both technical and human elements.

Dual-Use Technology Theory: This theory focuses on technologies that can be used for both beneficial and harmful purposes, directly relating to the dual-use nature of AI in cybersecurity. AI, while capable of defending systems, can also be misused to launch sophisticated cyberattacks. This dual-use dilemma reflects the inherent risks that accompany AI's transformative potential. The theory helps to explain the balancing act required to maximise the advantages of AI while preventing its misuse by malicious actors. Within this framework, AI's dual-use nature raises ethical and regulatory challenges and the need for responsible innovation in both the development and application of AI technologies in cybersecurity.

Technological Determinism: This theory posits that technology significantly shapes society, often driving social and organisational changes. When applied to AI in cybersecurity, technological determinism suggests that AI's evolving capabilities (e.g., processing vast datasets, automation of threat detection, and prediction of cyberattacks) are leading to structural changes in how cybersecurity is managed. AI is a tool and a driver of change that necessitates new governance models, ethical standards, and cybersecurity strategies.

Ethical and Regulatory Theories: The application of **deontological** or **utilitarian ethics** in the context of AI and cybersecurity also plays a crucial role in this framework. Deontological ethics would argue for clear rules and principles guiding AI's use in cybersecurity to avoid harm. In contrast, utilitarian ethics focuses on maximising benefits (enhanced security) while minimising risks (such as misuse or ethical violations). These ethical considerations emphasise the importance of developing frameworks that govern the responsible use of AI in cybersecurity, including addressing concerns about algorithmic bias, data privacy, and accountability.

Together, these theories provide a comprehensive framework for understanding AI's dual-use nature in cybersecurity. They highlight its potential benefits and risks, as well as the ethical and regulatory considerations that must be addressed to ensure its responsible use.

Cybersecurity

Several studies have explored the application of AI in cybersecurity, indicating that AIcan revolutionise the field by automating threat detection, improving incident response, and enhancing overall security measures (Buczak&Guven, 2016; Sommer&Paxson, 2010). However, alongside these opportunities, AI also introduces significant threats, such as the development of advanced malware, AI-powered cyberattacks, and the potential for AI systems to be exploited by malicious actors (Brundage et al., 2018; Huang et al., 2011). The existing literature reveals a growing concern about the dual-use nature of AI in cybersecurity, where the same technologies that protect systems can also be weaponised. Despite these concerns, there is limited research on the balance between leveraging AI's capabilities and mitigating its risks, particularly in rapidly evolving cyber environments. This chapter aims to bridge this gap by analysing the dual impact of AI on cybersecurity, providing a foundation for further exploration into how AIcan be harnessed effectively while minimising potential threats.

The literature reveals that AI holds substantial promise for enhancing cybersecurity through improved threat detection, predictive analytics, and automation, but it also introduces significant risks. AI's ability to be exploited for sophisticated attacks, along with ethical and regulatory challenges, underscores the need for ongoing research and policy development. Understanding these dynamics is crucial for developing effective strategies to harness AI's benefits while mitigating risks.

AI-Powered Threat Detection and Response:

AI's ability to analyse vast amounts of data in real-time makes it a powerful tool for threat detection. Techniques such as machine learning (ML) and deep learning can identify abnormal patterns in network traffic, detect zero-day vulnerabilities, and predict future threats based on historical data. This predictive capability goes beyond traditional rule-based systems, making AI indispensable in defending against rapidly evolving cyberattacks. For example, AI models can recognise ransom ware behaviour by detecting subtle signs before an attack occurs, leading to proactive rather than reactive security measures (Nguyen et al., 2018).

Automation of Incident Response:

AI has the potential to automate many aspects of incident response, reducing the response time and human error involved in countering cyber threats. AI-driven Security Information and Event Management (SIEM) systems can automatically respond to breaches, containing and mitigating damage without waiting for human intervention. This is particularly important given the sheer volume of cyber threats organisations face today, where manual responses may be too slow to prevent significant damage (Cruz et al., 2016).

AI as an Offensive Tool

While AI enhances defensive cybersecurity measures, its use as an offensive tool raises serious concerns. Malicious actors can harness AI to develop intelligent malware capable of adapting to different environments, evading detection, and launching autonomous attacks. **Adversarial AI** is a notable example, where attackers manipulate AI systems by introducing data designed to fool the algorithms, leading to incorrect predictions or classifications. For instance, hackers could introduce slightly modified images or data to bypass AI-based security systems (Biggio&Roli, 2018). AI can also scale social engineering attacks, such as generating deepfakes or using AIchatbots to carry out phishing attacks, making these techniques harder to detect and combat.

AI-Driven Cyberattacks and Autonomous Threats

AI systems themselves are vulnerable to attacks. **Adversarial machine learning** can trick AI models into misclassifying data, leading to inaccurate threat assessments or responses. AI-powered systems, once compromised, can be used to execute highly autonomous and persistent attacks. This poses a new challenge for cybersecurity experts, as such attacks can operate faster and more efficiently than traditional methods, making them harder to detect and mitigate. Moreover, **AI botnets**, which use AI algorithms to mimic human behaviour and continuously evolve to avoid detection, represent another emerging threat (Bendale&Boult, 2016).

The integration of AI into cybersecurity brings both promise and peril. On one hand, AI has the potential to revolutionise the field by improving threat detection, automating incident response, and enhancing overall security efficiency. On the other hand, it introduces significant risks, as malicious actors can weaponise the same AI technologies. As the literature indicates, balancing leveraging AI's capabilities and mitigating threats is crucial in modern cybersecurity. Furthermore, ongoing research, regulatory development, and ethical oversight are necessary to ensure that AIis used responsibly and effectively in cybersecurity contexts. As AI continues to evolve, its role in defending and threatening cyber systems will become an increasingly critical focus for researchers, practitioners, and policymakers alike.

Methods and Materials

Study Settings

The study will be conducted in various settings across industries such as finance, healthcare, government, and technology, where AI is actively integrated into cybersecurity measures. The survey will be distributed online via Google Forms to professionals in these sectors, ensuring ease of access and participation regardless of geographic location.

Research Approach

The research adopts a quantitative approach to gather measurable data from many respondents. This approach is ideal for understanding the prevalence and impact of AI technologies in cybersecurity by quantifying patterns, trends, and relationships. The data collected will focus on how much AI contributes to cybersecurity solutions and potential threats.

Research Design

An explanatory cross-sectional design is employed, focusing on gathering data at a single point in time. This design is well-suited for measuring current perceptions, practices, and outcomes related to the use of AI in cybersecurity. The cross-sectional nature allows for examining opportunities and threats as they exist in the present without requiring longitudinal follow-up.

Population Sample and Sampling Strategies

This study's target population consists of cybersecurity professionals, AI developers, I.T. managers, and experts directly involved in implementing or managing AI-driven cybersecurity systems. A purposive sampling strategy will be used to select participants with relevant experience. Invitations to participate in the Google Forms survey will be distributed through professional networks, social media platforms, and industry-related mailing lists.

Data Instrumentation

The primary data collection instrument is a structured survey hosted on Google Forms. The survey will include various question types designed to capture quantitative data on the impact of AI in cybersecurity. These include:

- **Multiple-choice questions:** To gather categorical data on the types of AI technologies used (e.g., machine learning, anomaly detection).
- **Likert-scale questions:** These are designed to measure perceptions of AI's effectiveness in enhancing cybersecurity and concerns regarding AI-induced vulnerabilities.
- **Yes/No questions:** To assess whether respondents have experienced AI-driven cyberattacks or system breaches.
- **Open-ended questions:** Although the survey is primarily focused on quantitative data, a few open-ended questions will allow respondents to share brief qualitative insights or specific examples of AI in their cybersecurity practices.

Data Collection Process

The survey will be designed and distributed using Google Forms, which offers several advantages:

1. **Ease of Distribution:** Invitations to complete the survey can be sent via email, social media, and professional platforms, allowing for a broad and diverse sample of participants.
2. **Automated Data Collection:** Responses are automatically logged, reducing the risk of data entry errors and ensuring efficient results collection.
3. **Anonymity and Confidentiality:** Google Forms allows for anonymous responses, ensuring that participants feel comfortable sharing their views, especially in cybersecurity, where privacy is paramount.

Survey Structure

The Google Forms survey will be divided into several sections to address the various aspects of AI's impact on cybersecurity:

1. Demographic Information: This section collects data on the participants' professional backgrounds, years of experience, and industry sector.
2. AI Technologies in Use: This section focuses on identifying the specific AI technologies that participants' organisations are using for cybersecurity purposes (e.g., machine learning algorithms, predictive analytics, and threat detection systems).
3. Opportunities from AI: Assesses how AI has improved cybersecurity practices in threat detection, response times, and overall system efficiency.
4. Threats from AI: This section examines whether AI introduces new cybersecurity risks, such as AI-driven phishing attacks, deep fake threats, or vulnerabilities in AI algorithms.
5. Ethical and Regulatory Concerns: This section captures respondents' views on the ethical implications of AI use in cybersecurity and the need for regulation or policy changes to address AI-related risks.

Data Analysis

The data collected from the Google Forms survey will be automatically compiled into a spreadsheet for analysis. Several analytical techniques will be used:

- **Descriptive Statistics:** This includes calculating frequencies, percentages, means, and standard deviations to summarise the data. For example, the percentage of organisations using specific AI technologies will be calculated to provide an overview of current industry practices.
- **Correlation Analysis:** Relationships will be explored between variables such as the type of AI technology used and perceived cybersecurity effectiveness.
- **Chi-Square Tests:** These will examine any significant associations between categorical variables, such as whether industries report different AI-driven threats.

Ethical Considerations

Before beginning the survey, participants will be informed of the purpose of the study and the anonymity of their responses. The Google Forms platform will not collect any personally identifiable information unless voluntarily provided by the respondent. Informed consent will be obtained through a pre-survey statement, ensuring that participants understand their rights, the purpose of the study, and how their data will be used. Additionally, participants will have the option to skip any questions they are uncomfortable answering.

Establishing the Information Base

The study began with an extensive literature review of current AI applications in cybersecurity. Relevant academic databases, journals, conference papers, and books were consulted to gather information on the benefits and challenges posed by AI in cybersecurity. Discussions with experts in AI and cybersecurity were also conducted to understand the current landscape better and shape the research questions and hypotheses.

In particular, sources such as peer-reviewed articles on AI-based cybersecurity strategies, reports from cybersecurity firms, and existing surveys on the adoption of AI in cybersecurity were invaluable in identifying the research gaps. This laid the groundwork for the survey instrument used in this study, which was designed to capture respondents' knowledge and experiences with AI-driven security systems, their perception of emerging AI-related threats, and the effectiveness of AI in mitigating cyber risks.

Survey Design and Instrumentation

A Google Forms-based survey was created to collect quantitative data from respondents. The survey was designed to include structured and semi-structured questions aligning with the research objectives and hypotheses. The instrument comprised sections on:

1. **Demographic Information**: To gather essential data about the respondents, such as their industry, role, and years of experience in cybersecurity.
2. **AI Tools and Applications in Cybersecurity**: Questions focused on the AI tools respondents have implemented or are aware of, their effectiveness, and how these tools have changed their cybersecurity strategies.
3. **AI-Driven Threats**: This section explored perceptions of AI as a tool for cybercriminals, including the types of AI-based threats they have encountered or anticipate encountering.
4. **Challenges and Risks**: This is a set of questions aimed at understanding respondents' key challenges when integrating AI into their cybersecurity frameworks.
5. **General Outlook on AI and Cybersecurity**: Respondents were asked about their overall perception of AI's future role in cybersecurity, weighing its opportunities and threats.

Sampling Strategy

The target population for this survey consisted of cybersecurity professionals with experience using AI technologies in their work. Convenience sampling was used to identify the participants, as the research aimed to reach a diverse range of individuals working in cybersecurity across different sectors. Respondents were recruited through professional networks, cybersecurity forums, and relevant LinkedIn groups. A target sample size of 200 professionals was set to ensure sufficient data for statistical analysis and generalisation.

Data Collection Procedure

The survey was distributed via email and social media, with participants invited to complete the Google Forms survey anonymously. To encourage participation, the survey was designed to take no more than 15 minutes to complete. Participants were given a two-week response window, with a reminder sent halfway through the period. All responses were collected in real-time through Google Forms, allowing immediate access to the data. The survey was kept open for an additional week to maximise the response rate.

Data Analysis

Once data collection was complete, the responses were downloaded from Google Forms and imported into Statistical Package for the Social Sciences (SPSS) for analysis. Data cleaning procedures were applied to ensure the accuracy and completeness of the dataset. Missing data were handled by excluding responses with more than 30% missing information.

The analysis included descriptive statistics to summarise the demographic data and inferential statistics to test the hypotheses. Key variables, such as the perceived effectiveness of AI tools and the degree of AI-driven threats experienced, were analysed using correlation and regression techniques to identify significant relationships.

Reporting the Results

The results will be presented in tables and graphs generated through SPSS. These visual representations will illustrate the distribution of responses and highlight key findings, such as the most commonly used AI tools in cybersecurity and the types of AI-driven threats cybersecurity professionals are most concerned about. A final report will be drafted to detail the research process, findings, and implications for the academic community and industry stakeholders.

Instrumentation

The survey for this study was designed to explore the impact of Artificial Intelligence (AI) on cybersecurity, with a particular emphasis on the opportunities and threats that AI presents. The survey comprised four subsections written in Standard English to ensure clarity and consistency, facilitate uniformity in responses, and streamline data analysis. Administered via Google Forms, the survey allowed for efficient data collection and management.

The first subsection, Demographic Information, aimed to collect fundamental details about the respondents. This section gathered information on the industry sector in which respondents are employed, their job roles, years of experience in cybersecurity, and their familiarity with AI technologies. This demographic data was essential for contextualising the responses and understanding the participants' backgrounds.

The second subsection, AI Adoption in Cybersecurity, focused on the extent of AI integration within respondents' cybersecurity practices. It sought to uncover the types of AI tools currently used, how frequently they are utilised, and respondents' perceptions of their effectiveness in enhancing cybersecurity measures. This section was crucial for assessing the current landscape of AI adoption and its impact on cybersecurity strategies.

The third subsection, Opportunities of AI in Cybersecurity, aimed to evaluate the positive impacts of AI within the field. Respondents were asked to describe the benefits of AI-enhanced security systems, such as faster threat detection and automated responses. This section also explored areas where AI has notably reduced vulnerabilities or bolstered overall system resilience and sought insights into the future potential of AI in addressing emerging cybersecurity challenges.

The final subsection, Threats of AI in Cybersecurity, investigated the potential risks and threats that AI might introduce. Questions in this section focused on AI-driven threats, such as AI-powered malware and adversarial attacks. Respondents were asked to share their experiences or observations of cybercriminals using AI and to discuss the challenges associated with defending against AI-based threats. This section was designed to provide a comprehensive understanding of the risks posed by AI and the difficulties in mitigating these threats.

By covering these areas, the survey provided a detailed examination of how AI influences cybersecurity, capturing both the opportunities for enhancing security and the potential threats that must be managed.

Survey Administration and Distribution

The survey was designed to be completed within **15 minutes** and was distributed online via Google Forms. Respondents were invited to participate through professional cybersecurity forums, LinkedIn groups, and direct outreach via email. The target population was cybersecurity professionals with experience or knowledge of AI technologies. **Convenience sampling**was used to recruit participants, ensuring diverse representation across different industries and job roles.

Data Entry and Processing

Once collected, the survey data were automatically captured and stored within Google Forms. The data was then exported to **SPSS** for analysis. A two-step process was followed to ensure data accuracy:

1. The research team performed **data validation**, ensuring completeness and correctness of the responses.
2. **Data cleaning**was conducted to handle any missing or incomplete data, with cases of over 30% missing data being excluded from the analysis.

Findings

Demographic Characteristics

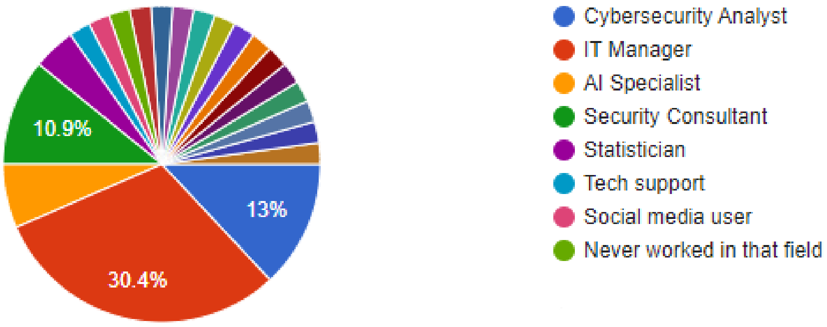


Figure 1: Current Occupations

Figure 1 depicts the current occupations of the respondents. Of the sample respondents, the majority were I.T. Managers (30.4%), followed by Cybersecurity (13%) and Security Consultants (10%).

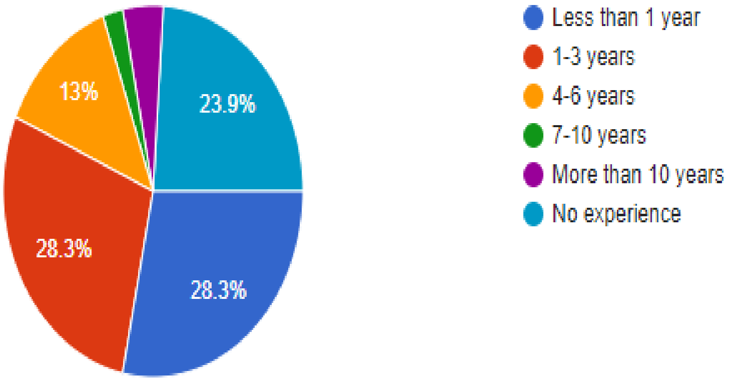


Figure 2: Work experience

Figure 2 depicts the work experience of the respondents. Of the sample respondents, the majority had 1-3 years and less than 1-year experience (28.3%), followed by 4-6 years of experience (13%) and no experience (23.9%).

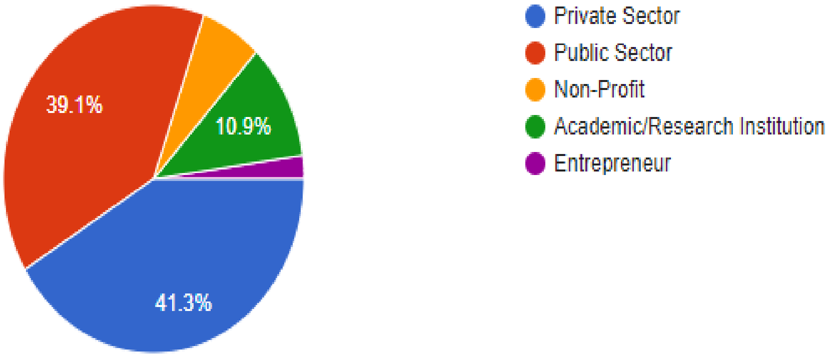


Figure 3: Different Organisations

Figure 3 depicts the different organisations. Of the sample respondents, the majority work in the Private Sector (41.3%), followed by the public sector (39.1%) and academic/research institutions (10.9%).

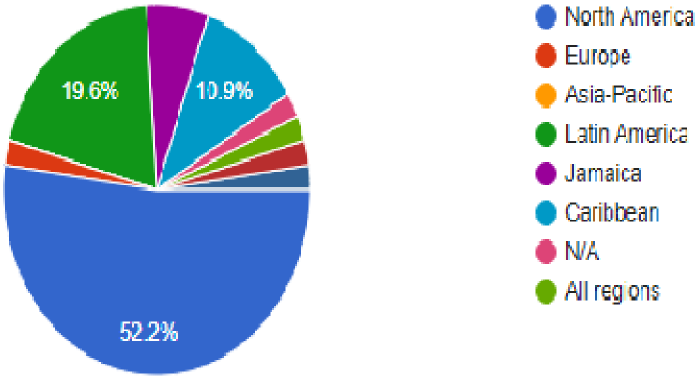


Figure 4: Regions

Figure 4 depicts the different regions in which the respondents are based. Of the sample respondents, the majority are based in North America (52.2%), followed by Latin America (19.6%) and the Caribbean (10.9%).

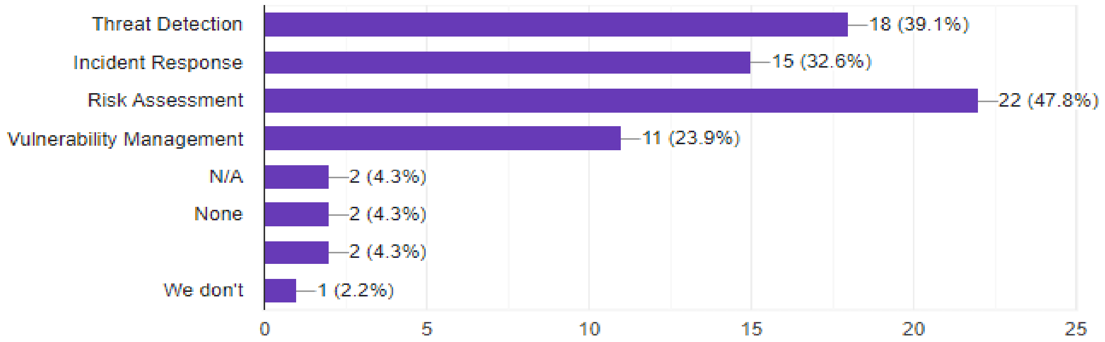


Figure 5: Areas of cybersecurity that organisationsuse.

Figure 5 depicts the areas of cybersecurity that organisations use. Of the sample respondents, the majority use cybersecurity for risk assessment (47.8%), followed by threat detection (39.1%), incident response (32.6%), and vulnerability management (23.9%).

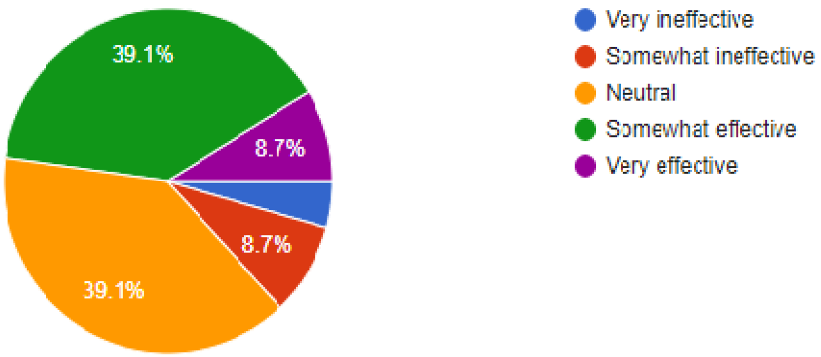


Figure 6: Effectiveness of AI in Enhancing Organizational Cybersecurity Posture

Figure 6 depicts the effectiveness of AI in enhancing organisational cybersecurity posture. Of the sample respondents, the majority said it is somewhat effective and neutral (39.1%), while others said it is somewhat ineffective and very effective (8.7%).

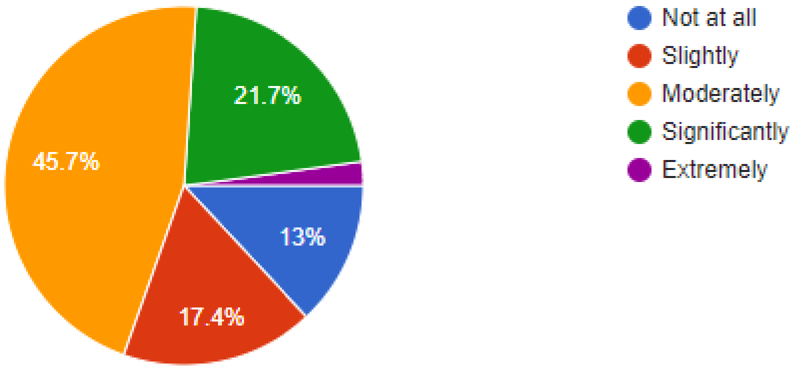


Figure 7: Extent to Which AI Has Enhanced Detection and Prevention of Cyber Threats in the Organization.

Figure 7 depicts the extent to which AI has enhanced the detection and prevention of cyber threats in the organisation. Of the sample respondents, the majority were moderate (45.7%), followed by significantly (21.7%), then slightly, and not at all (17.4% and 13%, respectively).

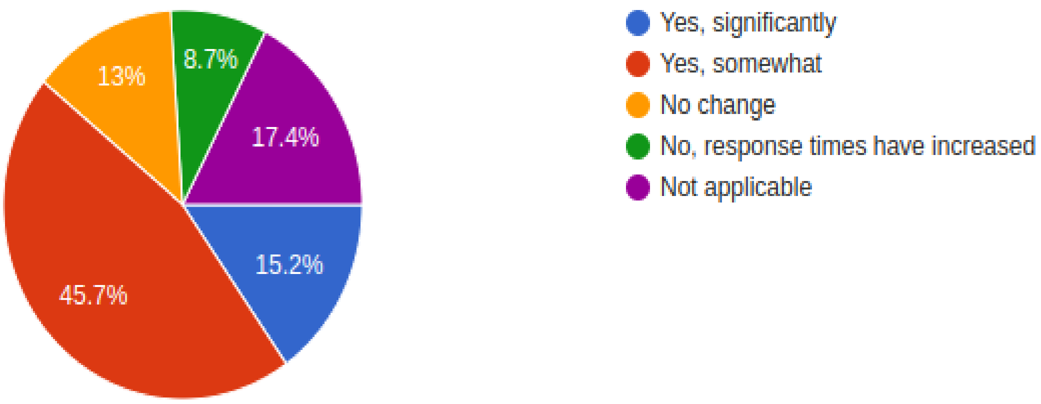


Figure 8: Impact of AI on Reducing Response Times to Cyber Incidents in the Organization

Figure 8 depicts the impact of AI on reducing response times to cyber incidents in the organisation. Of the sample respondents, the majority said yes, somewhat (45.7%), followed by not applicable (17.4%), then significantly, no change and response time increased (15.2%, 13%, and 8.7%, respectively).

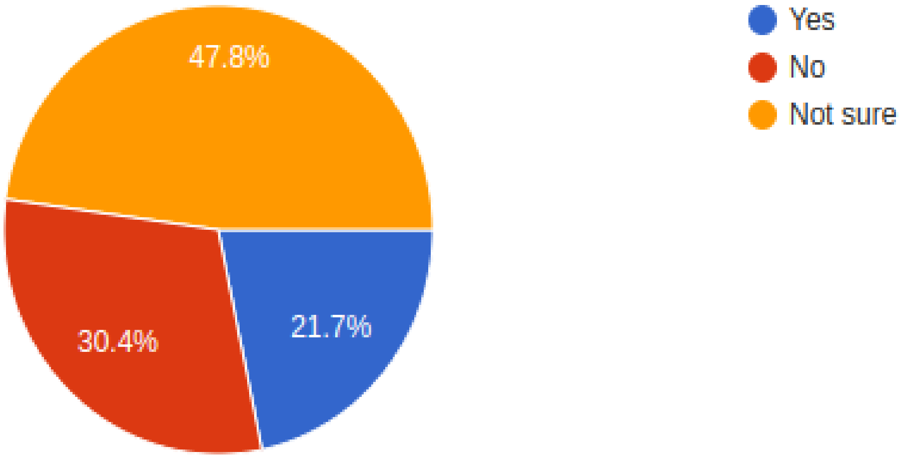


Figure 9: Incidence of AI-Driven Cyberattacks Experienced by the Organization

Figure 9 shows if there were any incident of any AI-Driven cyberattacks experienced by the organisation. Of the sample respondents, the majority of the respondents were not sure (47.8%) followed by No (30.4%) then Yes (21.7%).

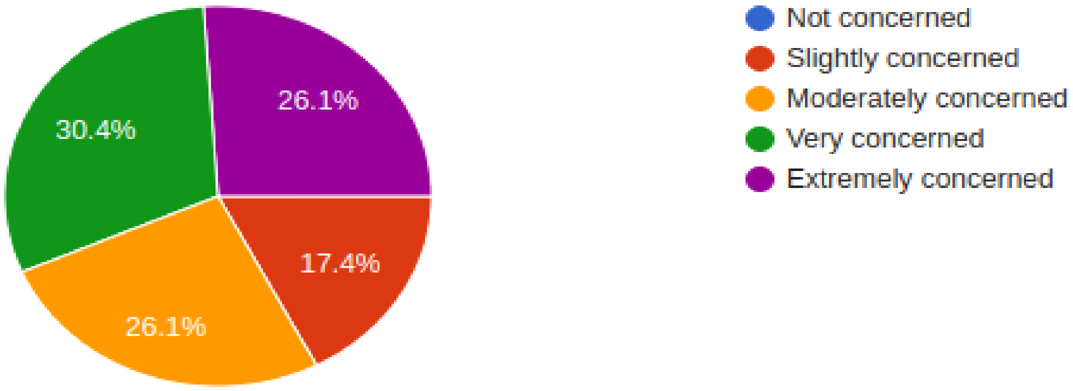


Figure 10: Concern About the Potential Misuse of AI by Cybercriminals.

Figure 10 depicts the concern about the potential misuse of AI by cybersecurity. Of the sample respondents, the majority were very concerned (30.4%) followed by moderately and extremely concerned (26.1%) then slightly concerned (17%).

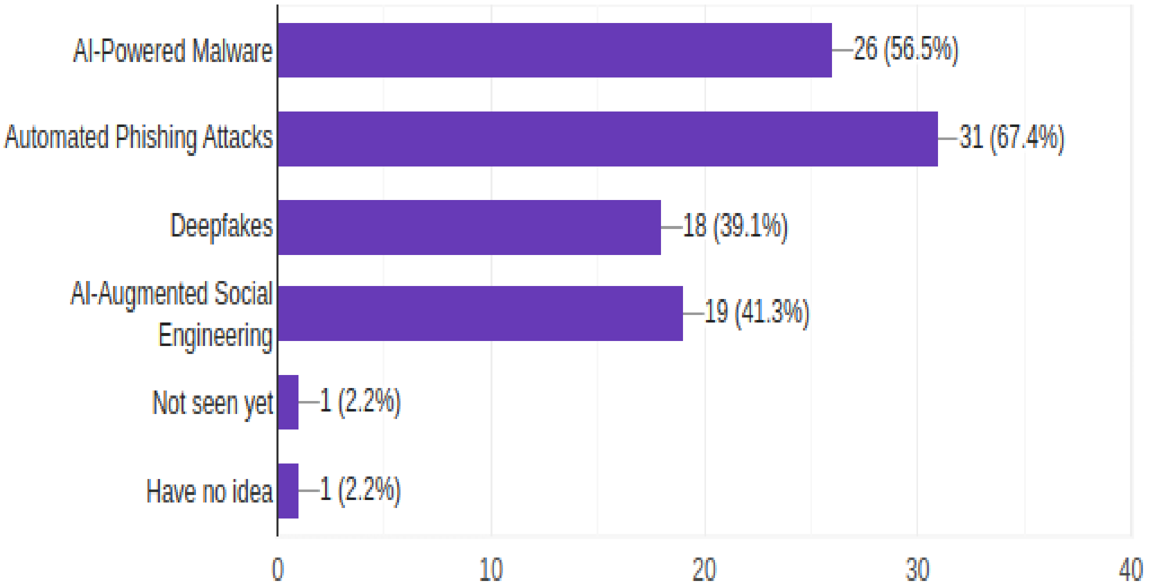


Figure 11: AI-Driven Threats Perceived as the Greatest Risk to Cybersecurity

Figure 1 depicts the AI-Driven threats that are the great risk to cybersecurity. Of the sample respondents, the majority were automated phishing attacks (67.4%) followed by AI powered malware (56.5%) then AI-augmented social engineering and deepfakes (41.3% and 39.1% respectively).

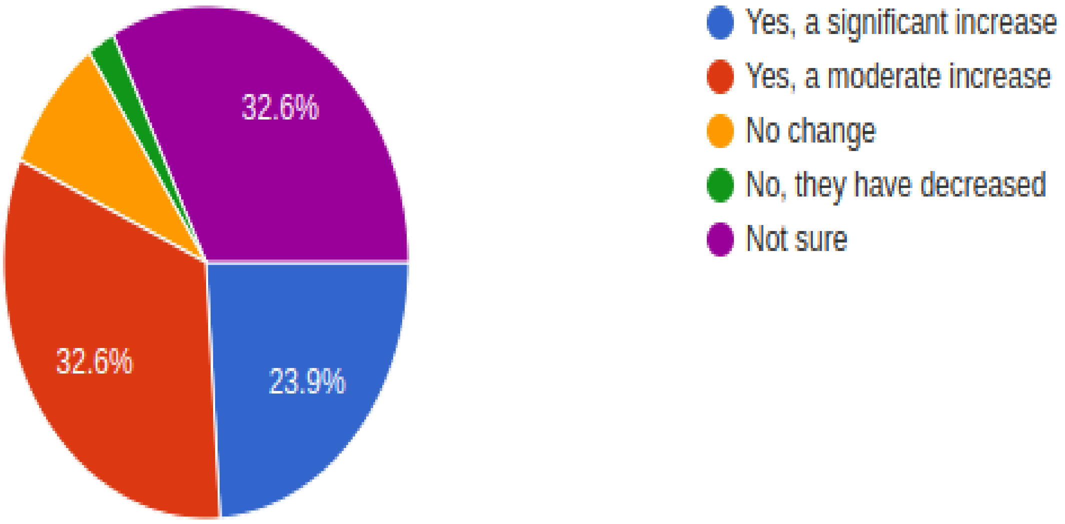


Figure 12: Increase in AI-Driven Cyberattacks in the Past 3 Years

Figure 12 shows whether there has been an increase in AI-driven cyber attacks in the past three years. Of the sample respondents, the majority were unsure and saw a moderate increase (32.6%) followed by a significant increase (23.9%).

Table 1: Greatest Threat AI Poses to Cybersecurity

Greatest Threat AI Poses to Cybersecurity
The greatest threat AI poses to cybersecurity is its potential use by malicious actors to automate and enhance cyberattacks. AIcan be leveraged to develop sophisticated phishing schemes, generate realistic fake content, and execute automated attacks with high precision. Additionally, AI-driven tools can be used to exploit vulnerabilities at scale, making it more challenging for traditional defenses to keep up. The ability of AI to adapt and evolve rapidly can significantly increase the sophistication and effectiveness of cyber threats.
Not sure
Not applicable
It may be easy to hack
Deepfake attacks, malware
Reliance on pre-trained models
At the rate at which AI is advancing, it has the potential to generate back doors/malware that are undetectable by the security systems currently employed by companies; the exploitation of these vulnerabilities can result in unauthorised access to sensitive data
I'm not sure
Phishing attacks
Exposure of data
It can be used for scam
The greatest threat that AI has posed was the ability for other persons to utilise AI to hack into cybersecurity.
Ethical problems, false positives/negatives, and malicious exploitation are major challenges in AI cybersecurity.
Machine learning and auto pattern change
In my opinion, AI poses the greatest threat to cybersecurity in terms of its skill in impersonation and identity theft
People taking their own life
Fraud Documents
Taking over everything without human knowledge.
Not informed about AI
N/a
Acting as actual humans
Takeover
Putting up hard-to-break firewalls and locking us out of the system completely
Automation
it adopts quickly
It can be hacked
Ease of creating fake profiles that can appear real
The greatest threat AI poses to cybersecurity is AI-powered cyberattacks. These attacks can be more sophisticated, adaptive, and difficult to detect.
data breaches, system compromises, or unauthorised access.
The use of AI to augment traditional attacks such as phishing
No comment
Smarter automated attacks and use of freely accessible information through social media and LLM prompts to perform sophisticated attacks based on information gained through insecure LLM prompting disclosing information and phishing or other social engineering attacks based on this information
advanced malware

Adaptability
Fakeness
Reliability
control
N/A
Malware
Enhanced Social Engineering, and Automated Intrusion deployments, with Algorithms used to exploit vulnerability (which can be implemented in a substantially short timeframe than human operators).
increase the risk
It helps well
Identity theft
N/A
More sophisticated attacks as AI learns at an alarming rate. Creating a lot of false positives in security checks etc.

Table 1 shows mixed feelings about the greatest threat that AI poses to Cybersecurity.

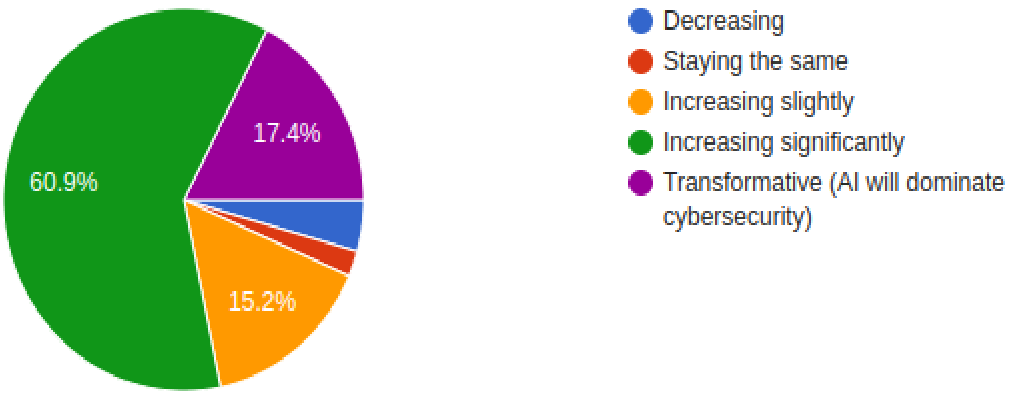


Figure 13: Future role of AI in cybersecurity in the next 5 Years.

Figure 13 depicts the future role of AI in cybersecurity in the next five years. Of the sample respondents, the majority would see a significant increase (60.9%), followed by transformative (AI will dominate cybersecurity) (17.4%), and then a slight increase (15.2%).

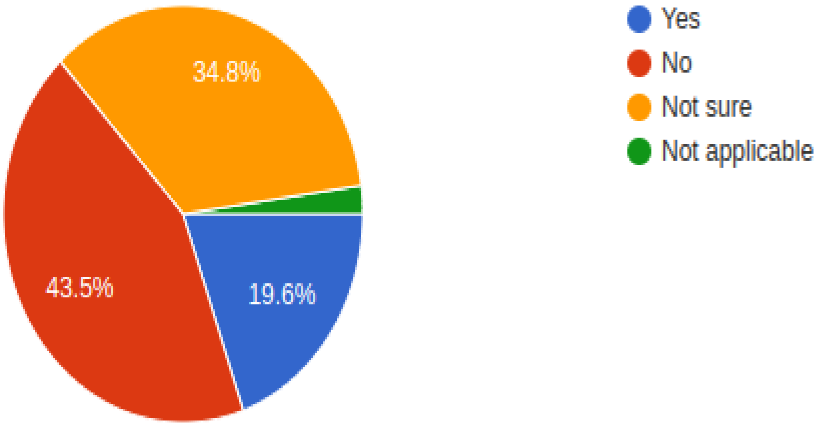


Figure 14: Adequacy of current Cybersecurity Policies and Regulations for addressing AI-related threats

Figure 13 depicts if the existing cybersecurity policies and regulations is adequate deal with the challenges and risks associated with AI technologies. Of the sample respondents, the majority said no (43.5%) followed by not sure (34.8%), then yes (19.6%).

Table 2: Recommendations for Policymakers to Enhance AI Regulation in Cybersecurity

Recommendations for Policymakers to Enhance AI Regulation in Cybersecurity
Develop Clear Standards and Guidelines: Establish comprehensive standards and guidelines for the ethical and secure development and deployment of AI in cybersecurity. This includes defining best practices for AI transparency, accountability, and data protection.
Employ persons to monitor cyber security
Not applicable
Strict fines and punishments for breaches
See to regular maintenance, respond to detections promptly
None at this time
Policy makers should keep abreast with the latest developments that take place with Artificial Intelligence to amend policies accordingly.
.
N/A
Not sure
Annual mandatory cybersecurity training
As stated in the previous question, policymakers should also invest more to improve the regulations. In addition, they should also be mindful of future events and how these regulations can affect later future if these regulations are not carefully analysed.
Policymakers must encourage collaboration between stakeholders, including researchers, developers, and end-users. They should also engage the public in discussions about AI technology to promote understanding, trust, and ethical considerations.
N/A
My specialty is not AItherefore I cannot formally speak on the reform of this issue.
Use it in a good way
Use AI in moderation.
I am not sure
Don't know
N/a
Stricter punishments
Get laws in line with the advanced technology
Make sure it's programed right. All the coding is top-notch for helping to fight against hackers
Null
Improve or incorporate AI related courses
Not sure
To create AI legislation that regulates the use of AI that is subject to disclosure, audits, sharing of third party information and compliance to data statutes
Enhance Training and Education: Invest in training programs to equip cybersecurity professionals with the skills needed to manage AI-driven tools effectively. Implement Robust Testing: Mandate rigorous testing and validation of AI systems to ensure they are secure, reliable, and free from biases.
To keep data fresh
Consult the field practitioners.
Understanding use and advantages of implementation
Difficult to say as many uses of AI weren't even thought about when the AI became a tool for use

so in the future use cases might evolve beyond current regulations as well
Provide and improve education and training to employees and other stakeholders on AI technologies, risks, regulations and best practices to ensure that they are well-equipped to, as well as identify and address AI-driven threats, follow and contribute to the development of relevant regulations.
Stay up to date with standards and software
Improved laws to prevent copyright
Make sure the AI is up to date and reliable
policy framework
Not sure
No recommendation
Start developing and implement rapidly charging policies to meet the growth and speed of AI Development, using AI tools to assist in addressing security risk.
CONDUCTING A RESEARCH INTO THE IMPACT
Not sure
Not sure
Have strict penalties for unethical and misuse of the technology
N/A
Develop markers to indicate AI use so it's clearly identifiable

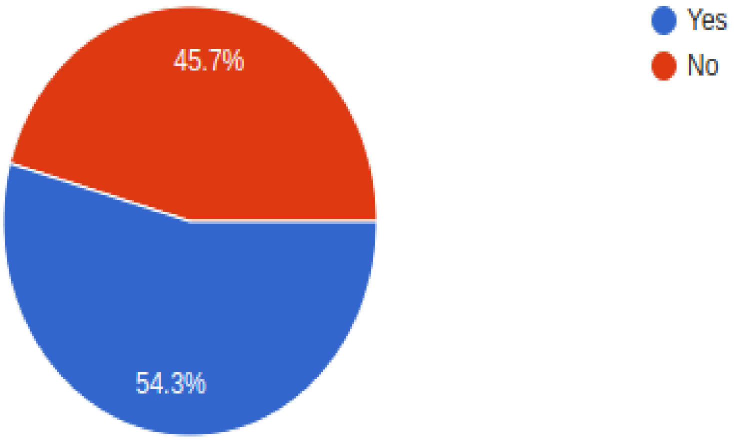


Figure 15: Interest in Receiving a Summary of the Study's Findings

Figure 15 shows how many respondents are interested in receiving a summary of the study. Of the sample respondents, No (45.7%) and yes (54.3%) are the most common responses.

General Research Question

Does integrating Artificial Intelligence in cybersecurity influence security measures and introduce new risks, particularly concerning adversarial attacks and ethical implications?

Specific Research Questions

This study aims to address the following key research questions:

Research Question One

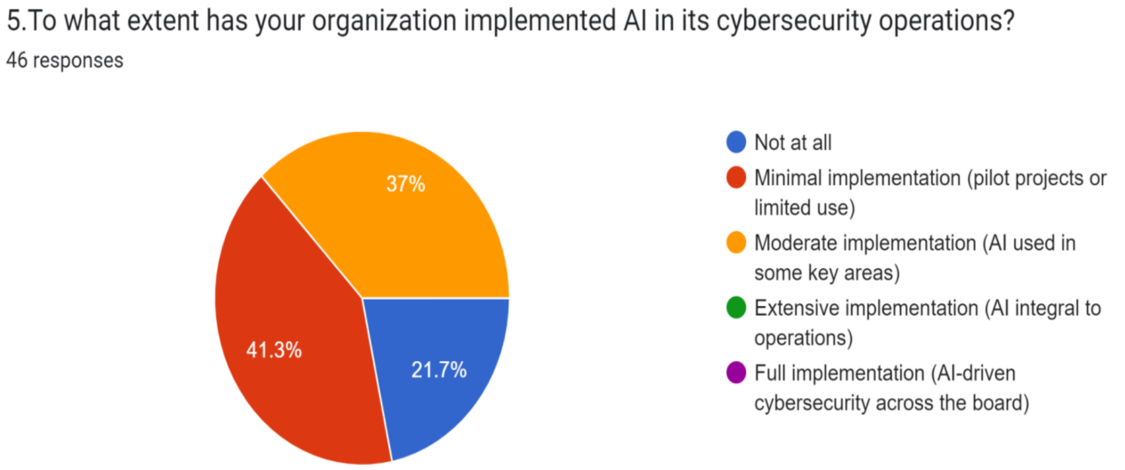
What are the primary opportunities that AI provides in the field of cybersecurity?

In my opinion, AI's greatest opportunity for cybersecurity is its ability to enhance threat detection and response through advanced pattern recognition and anomaly detection. AI systems can analyse vast amounts of data in real-time, identifying unusual behaviour or potential threats that might go unnoticed by traditional methods. This capability allows for faster identification of potential security breaches and can lead to more effective and proactive responses, ultimately improving overall security posture.
Provision of security in preventing crime
Allows machines to do human-like tasks
Less likelihood of major attacks
Efficiency and accuracy
Ability to train more than one model at a time to improve attack or threat detection
Artificial intelligence improves cyber security by enhancing and diversifying the range of responses and on a whole the measures that companies can implement to protect confidential information. A few ways would be Real Time Detection & Monitoring by scanning for unusual patterns/anomalies, thereby resulting in early detection. AI can also foresee vulnerabilities in a company’s security system by running security tests to ascertain the chances of common attacks to be successful.
Automation
Threat detection
Enhancing threat detection
Scam detection
The greatest opportunity that AI has presented was making work more efficient.
AI aids incident response by quickly analysing attacks, suggesting remediation steps, and automating responses to mitigate damage.
Automatic threat detection and response
In my opinion, AI allows for increased efficiency and proper examination of information, as a result it reduces the risks of threats and improves the protection of sensitive data flow.
I haven't used it yet
Better Efficiency
Knowledge and security improvements
It's not in my workplace
AI in cybersecurity can help with detecting threats &and abnormalities in the system.
More security
Better security
Faster response time, faster awareness of treats and better software coverage
Automation
I.T. cant indeed help with a faster response to cyber attracts
Going overseas to work with other people and learn new things
AI has the potential to provide better safety features that are foolproof and are better at detecting fraudulent access by using high-tech recognition systems.
The most significant opportunity AI presents for cybersecurity is enhanced threat detection. AI can analyse vast amounts of data in real-time, allowing organisations to detect and respond to threats more quickly and accurately.
Ability to analyse vast amounts of content and deliver insights,allowing security teams to detect and mitigate risk quickly and effectively.
AI would perhaps be most beneficial in risk assessment. It is uniquely able to remake evaluations based on training and make recommendations accordingly.
Intrusion detection and response
Similar to Recaptcha, it could be used to distinguish automated attacks from regular human

activity
zero-day threat detection/risk mitigation
Automated detections
Fakeness
Identify theft
verification
More protection of sensitive information
Efficiency
Enhance Treat Detection, Intrusion Prevention, and Point of Origin Lockdown.
it's both good and bad
It prevents hacking
It enables an organisationto detect threats automatically and can respond asap
Lower the human errors, and it is more accountable.
Protection
It more easily manages and sorts through mass data.

Research Question Two

How extensively are organisations adopting AI for cybersecurity purposes, and what factors influence its implementation?



5.To what extent has your organization implemented AI in its cybersecurity operations?

46 responses

Research Question Three

What future trends can be anticipated in the intersection of AI and cybersecurity?

Invest in Advanced Security Tools: Use AI-driven cybersecurity solutions to detect and respond to sophisticated threats in real time.
Creating safer software
Not applicable
Inform workers of the possible threats.
Perform more frequent system checks.
Training and plugging knowledge gaps of I.T. teams
1. Review existing policies and redefine procedures to reflect the necessary AI-specific security 2. Conduct exercises to identify potential threats to the security systems that are currently in place. 3. Access Management- Create policies that outline who can access data andprovide a guide for how data is to be classified,handled, maintained and disposed of.Furthermore, these

policies could include restrictions on data usage.
I'm not sure
Implementing and utilisingAI more for threat detection
N/A
Security training for employees
Organisations should try investing more funds to protect the confidentiality of their firms.
Employers can ease the disruption wrought by generative AIby providing high-quality training, dispensing clear guidelines on its use, and improving messaging about job security.
N/A
Ensure all activities performed using AIare overseen by trained professionals.
Do not ok overuse it
Limit and monitor the use of AI
I am not sure
Don't know
N/a
Get more advanced technology.
Adapt to climate
Either have some way to shut out AI hacks completely are built better protection software with good enough firewalls to keep them out
Educating employees on detecting potential threats
not sure
Not sure
Implement software programs that can detect AI fraud or malware.
Regular Updates: Ensure all AI and cybersecurity tools are regularly updated to protect against the latest threats. Employee Training: Conduct regular training sessions to educate employees about AI-driven threats and best practices.
Implementing (RBAC), (MFA)
AI-assisted threat handling.
Multilayer control practices
Implement policies to eliminate or reduce itsis or access to information unless the organisation controls the AI system and data
AI Education and Training with Incident Response Planning
Stay up to date with standards and software
Improved laws
Please make sure they are dependable.
threat framework
Developed a more secure system
Do not know
AI-enhanced firewall appliances, with key stakeholder training and interventions, more stringent update policies, and Penetration (Pen) Testing.
Be knowledgeable about AI
Let it stay the same
Use AIdefenthese
Routine debugging and monitoring
N/A
Invest in their employees keeping up with the latest AI development/trends.

Discussion

Artificial Intelligence (AI) is revolutionising the field of cybersecurity by providing several significant advantages, particularly advanced threat detection, AI-resilient strategies, thwarting AI-created vulnerabilities, and high responses to issues (Ilyas, 2024; Jada &Mayayise, 2024; Kaur et al., 2023; Kumar & Chandrashekar, 2020; Steele, 2024). The current study found thatthe majority use cybersecurity for risk assessment (47.8%), followed by threat detection (39.1%), incident response (32.6%), and vulnerability management (23.9%).AI can significantly enhance threat detection capabilities. The current study inquired whether there has been an increase in AI-driven cyberattacks in the past three years. Of the sample respondents, the majority were unsure and saw a moderate increase (32.6%) followed by a significant increase (23.9%).By analysing vast amounts of data in real-time, AI can identify unusual activity and potential threats that might escape human notice. Additionally, AI algorithms can learn to recognisemalicious behaviour patterns, allowing them to detect and prevent even the most sophisticated cyberattacks. Furthermore, AI can predict future cyber threats based on past data and current trends, enabling organisations to address vulnerabilities and mitigate risks proactively. Artificial intelligence can significantly enhance a company's cybersecurity capabilities. By automating routine tasks and prioritising critical threats, AI can help organisations respond to security incidents more quickly and effectively. In some instances, AI can even automatically fix vulnerabilities, reducing the risk of data breaches and other cyberattacks.

Findings from this research concurs with the literature that AI is associated with cybersecurity issues (Malatji&Tolah, 2024). This study examines whether AI's future role in cybersecurity will be in the next five years. Of the sample respondents, the majority indicated a significant increase (60.9%), followed by transformative (AI will dominate cybersecurity) (17.4%), and then a slight increase (15.2%) on the future role of AI in cybersecurity in the next five years.AI can significantly enhance an organisation's security posture by proactively identifying and mitigating vulnerabilities. It automates assessing networks, systems, and applications for weaknesses, allowing for targeted security measures. Additionally, AI helps ensure compliance with industry regulations and standards by efficiently checking for adherence and pinpointing areas needing attention. Moreover, by evaluating the potential risks associated with various threats, AI enables organisations to make strategic decisions regarding their security investments.Artificial intelligence can significantly enhance cybersecurity by analysing large amounts of data to detect patterns and trends indicating security threats (Jada &Mayayise, 2024; Kaur et al., 2023; Roshanaei et al., 2024). AI can also gather and analyse information about emerging threats from various sources, providing valuable insights to organisations (Jada &Mayayise, 2024; Kaur et al., 2023). Additionally, AI can generate comprehensive reports on an organisation's security posture, helping them understand their vulnerabilities and take proactive measures to protect their assets.

The current finding reveals that AI holds substantial promise for enhancing cybersecurity through improved threat detection, predictive analytics, and automation. However,it also introduces significant risks, which concur with the literature (Kalogiannidis et al., 2024; Mohamed, 2023). AI's ability to be exploited for enhanced attacks and ethical and regulatory challenges underscores the need for ongoing research and policy development. Understanding these dynamics is crucial for developing effective strategies to harness AI's benefits while mitigating risks.

Conclusion

In conclusion, artificial intelligence (AI) is a powerful tool that is useful in cybersecurity. However, its ability poses a risk if used unethically (enhanced attacks), which demands policy to safeguard its use. This requires a comprehensive strategy that includes public education on AI’s role in cybersecurity alongside evidence-based guidelines to manage the dual-edged nature of AI technologies. Understanding these dynamics is crucial for developing effective strategies to harness AI's benefits.

Recommendations

The findings of this dissertation have quantitatively established that cyber security'simpact on Artificial Intelligence has revolutionised our daily lives. So, the recommendations include:

General Knowledge

1. Educating the general public about cyber security awareness and Artificial Intelligence.
2. Implement measures to safeguard against common cyber security attacks (e.g., phishing).

This finding indicates the need for more public awareness about cyber security, which prevents them from knowing how to protect or defend themselves against cyber-attacks in this digital age.

Data Security

1. Protect the confidentiality, integrity and availability of the data being stored.
2. Data Security is the process of protecting data from unauthorised access (cybercriminals).

This finding indicates the importance of data security in cyber security. Data security is a safeguard for protecting an organisation or company's assets (data) from cybercriminals. Implementing these safeguards is fundamental for any company to survive in the digital age.

References

Anderson, R., & Moore, T. (2007). The economics of information security. *Science*, 314(5799), 610-613.

Awad, E., Dsouza, S., Kim, R., Schulz, J., Henrich, J., Shariff, A., Bonnefon, J. F., & Rahwan, I. (2018). The moral machine experiment. *Nature*, 563(7729), 59-64.

Biggio, B., Nelson, B., &amp; Laskov, P. (2018). Poisoning attacks against support vector machines.arXiv preprint arXiv:1206.6389.

Binhammad, M., Alqaydi, S., Othman, A. and Abuljadayel, L. H. (2024). The Role of AI in Cyber Security: Safeguarding Digital Identity. *Journal of Information Security*, 15, 245-278. doi: 10.4236/jis.2024.152015.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ...&Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Buczak, A. L., &Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153-1176.

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys &amp; Tutorials, 18(2), 1153-1176.

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': The U.S., E.U., and U.K. approach. *Science and Engineering Ethics*, 24(2), 505-528.

Chandramouli, R., Grance, T., &amp; Ferraiolo, D. (2020). NIST cybersecurity framework: Acomprehensive guide to best practices (2nd ed.). CRC Press.

Check Point Team. (2024, July 15). Check Point Research Reports The highest increase in global cyber attacks seen in the last two years was a 30% increase in Q2 2024 global cyber attacks. https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

Chowdhury, F., Iqbal, A., & Rahman, A. (2019). Enhancing phishing email detection using natural language processing techniques. In *2019 International Conference on Electrical, Computer and Communication Engineering* (pp. 1-6). IEEE.

De Azambuja, A. J., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0-A Survey. *Electronics*, *12*(8), 1920. https://doi.org/10.3390/electronics12081920.

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608.*

Dunsin, D., Ghanem, M. C., Ouazzane, K., &Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, *48*, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., Kalogeratos, G., &Tsolis, D. (2023). Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. *Journal of Cybersecurity and Privacy*, *3*(3), 493-543. https://doi.org/10.3390/jcp3030025

Gonzalez, R. (2020). AI and cybersecurity: A race between hackers and defenders. IEEESecurity &amp; Privacy, 18(1), 82-85.

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). She was explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572.

Hassan, W. U., Bates, A., &amp; Wang, D. (2019). Towards scalable cluster auditing through grammatical inference over provenance graphs. In 2019 IEEE Symposium on Security and Privacy (S.P.) (pp. 1275-1294). IEEE.

Hong Kong Computer Emergency Response Team. (2024, July 10). *Weaponisation of AI: The New Frontier in Cybersecurity*. https://www.hkcert.org/blog/weaponisation-of-ai-the-new-frontier-in-cybersecurity

Huang, C., & Zhu, J. (2019). Adversarial machine learning: A security perspective. *Journal of Physics: Conference Series*, 1237(2), 022082.

Ilyas, M. (2024). Revolutionizing Cybersecurity: The Role of Artificial Intelligence in Advanced Threat Detection and Response. *International Journal of Applied Mathematics and Computer Science*, 3(7), 77-85.

Interpol. (2020). *Cybercrime: COVID-19 impact*. Interpol.

Jada, I., &Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, *8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Kalogiannidis, S., Kalfas, D., Papaevangelou, O., Giannarakis, G., &Chatzitheodoridis, F. (2024). The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece. *Risks*, *12*(2), 19. https://doi.org/10.3390/risks12020019

Kaur, R., Gabrijelčič, D., &Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804.

Kietzmann, J., Lee, L. W., McCarthy, I. P., &amp; Kietzmann, T. C. (2020). Deepfakes: Trick ortreat? Business Horizons, 63(2), 135-146.

Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690-1700.

Kumar, S., & Chandrashekar, D. (2020). Deepfake: A looming challenge for cybersecurity. *Journal of Cyber Security Technology*, 4(4), 247-259.

Kurakin, A., Goodfellow, I., & Bengio, S. (2017). Adversarial examples in the physical world. *arXiv preprint arXiv:1607.02533*.

Malatji, M., &Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI*AI Ethics*. https://doi.org/10.1007/s43681-024-00427-4.

Mitchell, T. M. (1997). *Machine learning*. McGraw-Hill.

Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, 10(2). https://doi.org/10.1080/23311916.2023.2272358.

Osasona, F., Amoo, O.O., Atadoga, A. Benjamin Samson Ayinla, B.S., et al. (2024).Reviewing the Ethical Implications of AI in Decision-Making Processes. International Journal of Management & Entrepreneurship Research 6(2):322-335. DOI: 10.51594/ijmer.v6i2.773

Rigaki, M., & Garcia, S. (2020). Bringing a GAN to a knife-fight: Adapting malware communication to avoid detection. In *2018 IEEE Security and Privacy Workshops* (pp. 70-75). IEEE.

Roshanaei, M., Khan, M. R. &Sylvester, N. N. (2024) Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions. *Journal of Information Security*, **15**, 320-339. doi: 10.4236/jis.2024.153019.

Russell, S. J., &amp; Norvig, P. (2016). Artificial intelligence: A modern approach (3rd ed.). Pearson Education.

Sharma, N., &Dua, A. (2020). Predictive analytics in cybersecurity: Role of machine learning. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering* (pp. 324-329). IEEE.

Sommer, R., &amp; Paxson, V. (2010). Outside the closed world: On using machine learning fornetwork intrusion detection. In 2010 IEEE Symposium on Security and Privacy (pp. 305-316).IEEE.

Steele, G. (2024, January 15). Cybersecurity is on the frontline of our AI future. Here's why. World Economic Forum. https://www.weforum.org/agenda/2024/01/cybersecurity-ai-frontline-artificial-intelligence/

Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*.

Types of cybersecurity. (2023). SailPoint. https://www.sailpoint.com/identity-library/five-types-of-cybersecurity

World Economic Forum. (2020). *The Global Risks Report 2020*. World Economic Forum. https://www.weforum.org/publications/the-global-risks-report-2020/