International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity

Chris Gilbert[1], Mercy Abiola Gilbert[2], Maxwell Dorgbefu Jnr[3], Duah Jeremiah Leakpor[4], Kwitee D. Gaylah[5], Isaac A. Adetunde[6]
[1, 4, 5, 6]Department of Computer Science and Engineering/College of Engineering and Technology, William V.S. Tubman University
[2]Department of Guidance and Counseling/College of Education, William V.S. Tubman University/
[3]Department of Information Technology Education, Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED), Ghana
Corresponding Author Email Address: cabilimi@tubmanu.edu.lr

Abstract*—This paper examines the transformative potential of artificial intelligence (AI) in enhancing cybersecurity, particularly within Security Operations Centers (SOCs). By integrating advanced machine learning and deep learning techniques, AI is shown to augment human expertise in detecting and responding to cyber threats more effectively than traditional rule-based systems. Through an extensive literature review, comparative analysis, and real-world case studies including applications in ChatOps, DDoS mitigation, speech recognition, and image captioning the study demonstrates how AI can process vast amounts of security data to reduce false positives and shorten incident response times. The findings reveal that while AI significantly improves operational efficiency and threat detection, its integration also introduces technical challenges and ethical concerns, such as algorithmic bias and privacy issues. The paper concludes with strategic recommendations for embedding AI within existing cybersecurity frameworks and outlines future research directions focused on advanced AI models, natural language processing, and adaptive security strategies*.

Keywords: *Artificial Intelligence, Cybersecurity, Machine Learning, Deep Learning, Security Operations Centers, Threat Detection, Incident Response, SOAR Platforms, Ethical Considerations, Adaptive Security Models*.

I. INTRODUCTION

In today's increasingly complex threat landscape, artificial intelligence (AI) is emerging as a transformative asset for enterprise defense (Manoharan & Sarker, 2023; Gilbert & Gilbert, 2024b; Khan et al., 2024). Rather than supplanting security analysts, AI functions as an effective co-helper streamlining the arduous, subjective, and error-prone processes currently prevalent in Security Operations Centers (SOCs) (Gilbert & Gilbert, 2024c). By ingesting, reviewing, and analyzing vast streams of security log data with unprecedented speed and accuracy, AI significantly reduces the time between an initial breach and the corresponding response, thereby mitigating risk and curbing potential economic losses (Singh, 2024; Gilbert & Gilbert, 2024a).

Leveraging expert knowledge and its capacity to learn autonomously from continuous streams of cyber data, AI is capable of making informed decisions with minimal human intervention (Alsamhi et al., 2024; Gilbert & Gilbert, 2024d). This scalability and depth of analysis help address the inherent limitations of conventional SOCs, where the manual review of alerts is labor-intensive and prone to error. Users are encouraged to integrate AI into their SOC tools not only to handle explicit alert representations but also to unearth subtle anomalous behaviors and data patterns that might otherwise go unnoticed (Mokhtarian, 2024; Gilbert & Gilbert, 2024i; Surampudi, 2024; Markowitz, Boyd & Blackburn, 2024).

Given the persistent threat posed by sophisticated adversaries, organizations must assume that breaches are inevitable and reconfigure their security architectures accordingly (Christopher, 2013; Gilbert & Gilbert, 2024f). While existing SOCs provide alerts based on known threat behaviors, these systems still depend on human expertise to interpret and analyze the data (Gilbert & Gilbert, 2024e). Consequently, the human element introduces potential for subjectivity and error. As attackers increasingly breach defenses undetected and operate covertly for extended periods, the need for AI-enhanced detection and response mechanisms becomes ever more critical (Gilbert & Gilbert, 2025b).

This diagram shows how modern Security Operations Centers (SOCs) can evolve from manual processes, which are time-consuming and prone to human error, to AI-driven methods that greatly accelerate data ingestion, anomaly detection, and incident response. By automating much of the review process, AI helps teams quickly sift through massive data sets and pinpoint suspicious activities with minimal human oversight, reducing both risk and economic losses. Furthermore, AI can serve as a co-helper, streamlining traditionally subjective tasks and addressing the limitations of conventional SOC operations. When AI is integrated into existing SOC tools, it not only handles explicit alerts more effectively but also uncovers subtle anomalies that might otherwise go unnoticed.

II. BACKGROUND AND SIGNIFICANCE OF AI IN CYBERSECURITY

This paper examines how artificial intelligence (AI) is transforming cybersecurity, particularly in the cyber battlefield. AI is no longer limited to simply detecting patterns, threats, or vulnerabilities it now plays an active role in quickly identifying threat signatures and initiating early

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

remediation, a capability essential for the Department of Defense to operate at machine speed (Dhayanidhi, 2022; Gilbert & Gilbert, 2024g). Moreover, AI has moved beyond being a problem confined to large computer systems; it is now embedded at the tactical edge within its own hosting environments.

Recent cybersecurity incidents, such as WannaCry, NotPetya, and a subsequent variant sometimes referred to as WannaCry 2.0, highlight the shortcomings of traditional, signature and rule-based defenses (Abdelkader et al., 2024; McCoy, 2022; Gilbert & Gilbert, 2024h; Bhardwaj, 2024; Chakraborty, Biswas & Khan, 2023). These incidents demonstrate the heavy costs and serious repercussions of relying on outdated systems and protocols that fail to address vulnerabilities stemming from inadequate software, misconfigured user access, and other oversights (Sontan & Samuel, 2024; Gilbert & Gilbert, 2024j).

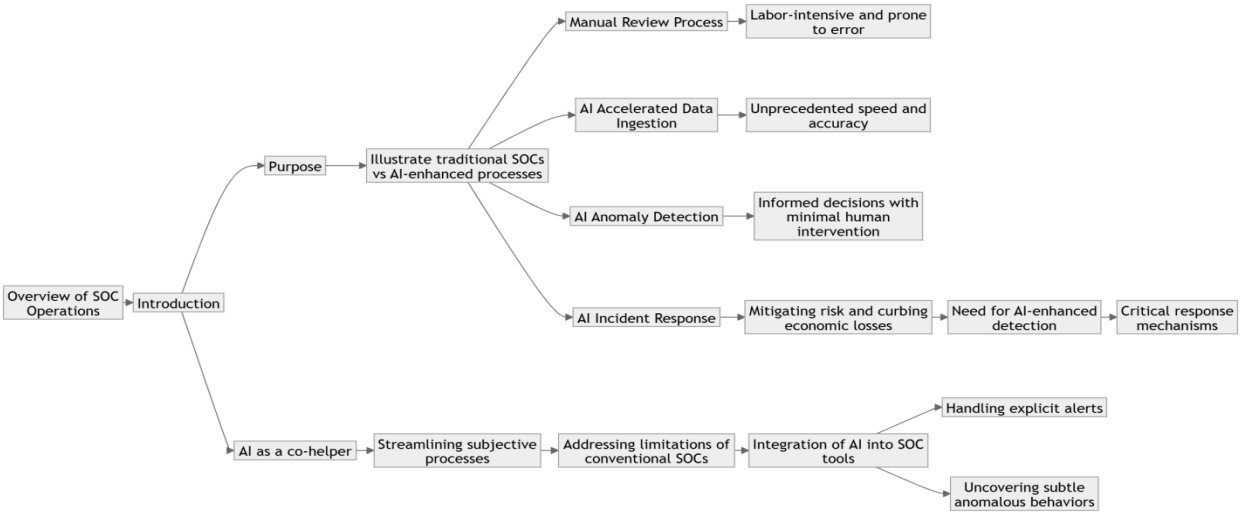

Figure 1: An overview of Security Operations Center (SOC) activities.

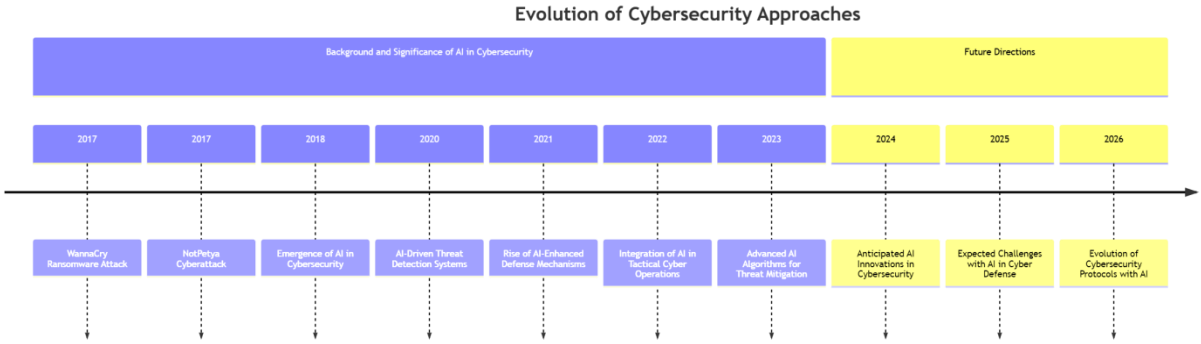

Figure 2: How AI has become increasingly central to cybersecurity between 2017 and 2023, and then looks ahead to future directions from 2024 onward.

Looking forward, while AI brings impressive strengths to the table, it also introduces unique risks that must be managed. AI is not just enhancing cybersecurity; it is reshaping how cyber threats are disclosed and discussed.

As we transition into an era where billions of connected 'citizens' and 'things' communicate with each other, the need for secure and resilient data networks becomes ever more critical. From a military perspective, maintaining a battle-ready network requires a balance of security, agility, resiliency, scalability, and adaptability (Edmund & Enemosah, 2024; Gilbert & Gilbert, 2025a). This evolution is evident in the shift from traditional technical approaches dominated by signature and rule-based solutions to advanced, AI-driven methods that employ sophisticated mathematics, algorithms, machine learning, and AI technologies (Jimmy, 2024; Gilbert & Gilbert, 2024k).

This timeline shows AI's growing role in cybersecurity, starting with major cyberattacks in 2017 that exposed vulnerabilities and sparked interest in AI-driven defenses. By 2018, early machine learning applications emerged, and between 2019 and 2020, AI-powered threat detection became more advanced, improving automated responses. From 2021 to 2022, AI began playing a bigger role in tactical cyber operations and threat mitigation. By 2023, AI innovations were enhancing real-time detection and adaptive countermeasures. Looking ahead, 2024 and beyond will bring new challenges and advancements in AI-driven cybersecurity. By 2025 and later, AI is expected to be deeply integrated into

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

threat detection, prevention, and response, shaping the future of cybersecurity protocols.

III. Research Objectives

The objectives of this paper are to:

i. Investigate how artificial intelligence, particularly through machine learning and deep learning techniques, can be integrated into Security Operations Centers (SOCs) to augment threat detection and streamline incident response.
ii. Evaluate the performance improvements offered by AI-driven systems over traditional, rule-based defenses.
iii. Analyze the technical, ethical, and operational challenges associated with deploying AI in cybersecurity.
iv. Synthesize Best Practices and Case Study Insights drawing from existing case studies and real-world implementations to outline best practices for integrating AI into cybersecurity.
v. Propose a conceptual and practical framework that maps out how AI can be effectively embedded within existing cybersecurity architectures.

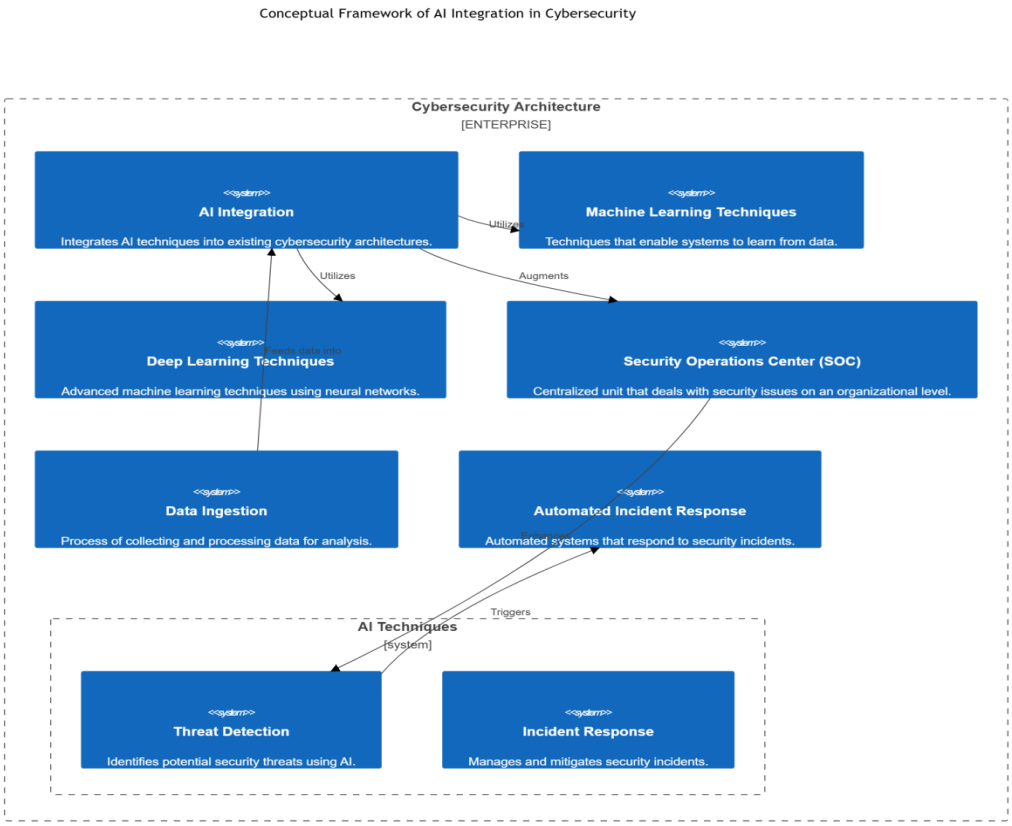

Figure 3: An Enterprise Cybersecurity Architecture powered by AI-driven techniques.

This diagram outlines an AI-powered cybersecurity framework for enterprises, showing how machine learning and automation enhance security operations. AI is integrated into various processes, allowing systems to continuously learn, detect threats, and respond to incidents in real time. At the core of this framework is the Security Operations Center (SOC), which oversees security threats and manages automated responses. Machine learning and deep learning techniques analyze vast amounts of security data, while data ingestion ensures a steady flow of information for threat detection. AI-driven threat detection identifies risks early, and automated incident response quickly mitigates threats before they escalate. Through integrating AI into cybersecurity, organizations can improve detection speed, reduce response times, and strengthen overall security, making defenses more adaptive and proactive.

IV. Research Questions

I. How does AI integration improve threat detection and response compared to traditional rule-based methods?
II. What are the specific contributions of machine learning and deep learning algorithms to enhancing cybersecurity measures?
III. What are the major challenges, including ethical concerns, that arise when integrating AI into cybersecurity systems?
IV. In what ways can AI be seamlessly integrated into existing SOCs to optimize incident detection and response?

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

V. What lessons can be learned from current case studies and real-world implementations of AI in cybersecurity, and how can these lessons inform future research and practices?

V. Research Methodology

The research methodology for this study was designed as a multi-step, integrative process, combining comprehensive literature analysis, comparative evaluation, and real-world case studies to arrive at the findings and conclusions.

i. Extensive Literature Review and Framework Development

The study began with an in-depth review of academic journals, industry reports, and technical documents related to both traditional cybersecurity measures and the emerging role of artificial intelligence (Ozkan-Okay et a., 2024; Gilbert & Gilbert, 2024l). This phase established a solid theoretical foundation by:

a. Examining the limitations of existing Security Operations Centers (SOCs).
b. Exploring various AI approaches such as machine learning, deep learning, and heuristic methods.
c. Identifying gaps in current cybersecurity practices that AI could potentially address.

ii. Comparative Analysis of AI-Driven and Traditional Methods

Researchers conducted a side-by-side comparison of conventional, rule-based cybersecurity defenses with AI-enhanced techniques (Salem et al., 2024; Gilbert & Gilbert, 2024m). This comparison focused on:

a. Evaluating improvements in threat detection speed and accuracy.
b. Measuring the reduction in false positives and overall response times.
c. Analyzing how AI systems process vast amounts of security data compared to manual reviews.

iii. Real-World Case Study Evaluation

The methodology incorporated a detailed examination of various case studies, which served as practical examples of AI integration in cybersecurity (Kaur, Gabrijelčič & Klobučar, 2023; Sarker, Furhad & Nowrozy, 2021; Malatji & Tolah, 2024). These case studies included:

a. ChatOps for Cybersecurity: Using chat-based tools to streamline and record security operations.
b. Deep Learning for DDoS Mitigation: Implementing reinforcement learning for dynamic load balancing.
c. Speech Commands Recognition and Image Captioning: Applying advanced AI techniques to enhance data processing and analysis.
d. By reviewing these real-world applications, the study was able to draw best practices and operational insights.

iv. Synthesis and Conceptual Framework Development

Findings from both the literature review and case studies were synthesized to develop a comprehensive conceptual framework (Zhang et al., 2022). This framework:

a. Maps out how AI can be effectively embedded within existing cybersecurity architectures.
b. Provides strategic recommendations for integrating AI into SOCs.
c. Addresses technical, ethical, and operational challenges identified during the analysis.

v. Iterative Analysis and Expert Validation

Throughout the research process, the findings were continuously refined through iterative analysis and feedback from industry experts (AL-Dosari, Fetais & Kucukvar, 2024). This step ensured that:

a. The conclusions were not only based on theoretical research but also on practical, real-world insights.
b. The recommendations were both innovative and feasible for modern cybersecurity challenges.

This integrative methodology allowed the researchers to rigorously evaluate the transformative impact of AI in cybersecurity, culminating in actionable findings and a forward-thinking framework for future implementation.

This research framework compares AI-driven and traditional cybersecurity methods to assess their effectiveness in threat detection and incident response times. It begins with a literature review and framework development, followed by a comparative analysis of both approaches. Real-world case studies, such as ChatOps for cybersecurity, deep learning for DDoS mitigation, and speech command recognition, provide practical insights into AI's impact. These findings are synthesized into a conceptual framework, leading to strategic recommendations. The framework is then refined through iterative analysis and expert validation, ensuring a well-rounded evaluation before concluding the study.

VI. Fundamentals of Cybersecurity

Weak security infrastructures or outdated antivirus solutions can offer intruders an opening to execute malicious activities (Mohammadi, Hosseini & Bahrami, 2025; Gilbert & Gilbert, 2024n). As Internet connectivity and networking technologies proliferate, defense systems often struggle to remain fully robust (Aslan et al., 2023; Gilbert & Gilbert, 2024o). Modern computer security measures frequently fall short when protection is minimal, and it is important to acknowledge that no system is entirely impervious. Even when a computer system is well-protected, its security policies may be compromised during the development process (Gilbert & Gilbert, 2024p).

The methods attackers use ranging from virus propagation via email to exploiting intrusion detection systems and installing backdoors highlight the critical importance of securing computer systems (Mohammadi, Hosseini & Bahrami, 2025; Gilbert & Gilbert, 2024q). To mitigate these risks, it is essential to design software with integrated security functions aimed at minimizing or preventing vulnerabilities. Security functions serve as checkpoints within a system, monitoring for potential breaches. In cases where software exhibits non-functional vulnerabilities, structured error-analysis models can be employed to track all states and transitions, ensuring that vulnerable conditions are identified and addressed (Sharma et al., 2022; Gilbert & Gilbert, 2024r).

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

Some security functions come with enhanced features such as immutability, fault tolerance, and information hiding, which further strengthen a system's defenses (Gilbert & Gilbert, 2024s; Aslan et al., 2023). Conversely, vulnerabilities like unchecked input parameters, unpredictable interfaces, and invalid function calls represent significant threats if not managed properly.

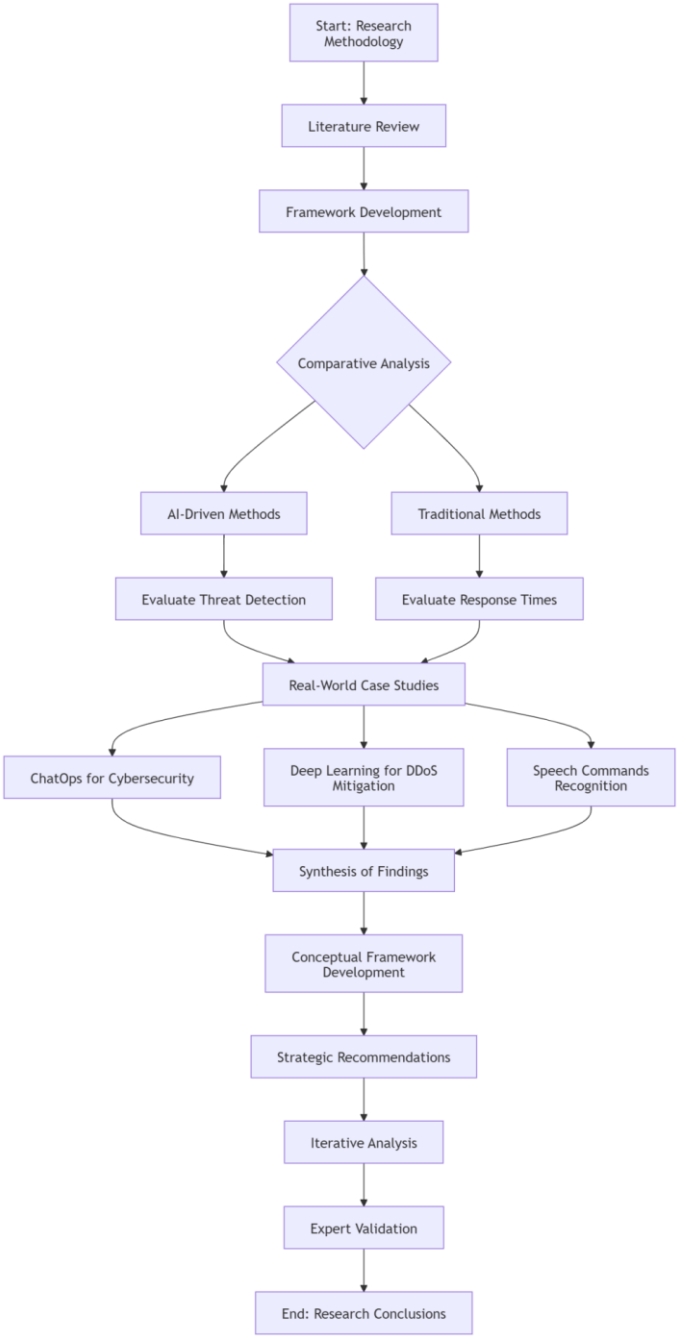

Figure 4: A research methodology for comparing AI-driven cybersecurity methods with traditional security approaches.

Cybersecurity is vital for maintaining both the safety and efficiency of our digital world. The complexity of protecting cyber environments can involve significant financial and temporal resources, and even robust systems are not entirely immune to failure (Gilbert & Gilbert, 2024t; Safitra, Lubis & Kurniawan, 2023). Effective risk management requires continuous reassessment such as annual reviews of cyber-risk exposure and regular updates to mitigation policies (Tzavara & Vassiliadis, 2024; Gilbert & Gilbert, 2024u). Importantly, cybersecurity is not solely a technological challenge but also a management issue, where proper risk management strategies must integrate technology and policy (Gilbert & Gilbert, 2024v; Linkov & Kott, 2019). Successful cybersecurity practices depend on the collective efforts of all stakeholders from employees and developers to managers ensuring that security measures support the confidentiality, integrity, and availability of information resources (Cofer et al., 2022; Gilbert & Gilbert, 2024x). Ultimately, robust information security practices are essential to minimize disruptions and secure the optimal functioning of organizations.

6.1. Key Concepts and Terminologies

Artificial Intelligence (AI) refers to machines designed to behave in ways that we would consider intelligent (Shin & Xu, 2017; Gilbert & Gilbert, 2024y). In practice, applying AI to solve a specific problem involves building models, learning from data, reasoning through complexities, and taking actions suited to the situation at hand (Hopgood, 2021; Gilbert, Auodo & Gilbert, 2024). There isn't just one way to achieve AI; rather, there are various theories and paradigms such as rule-based systems, case-based reasoning, pattern recognition, neural networks, and probabilistic reasoning—that each target different implementation goals (Yazici, Shayea & Din, 2023; Gilbert. Oluwatosin & Gilbert, 2024).

Today, AI developments generally fall into three main categories: machine learning (ML), knowledge-based AI (KB AI), and evolutionary or emergent AI (Vu et al., 2024; Gilbert, 2012). AI tools have already shown impressive results by performing tasks in ways that resemble human intelligence (Gilbert, 2022; Sarker et al., 2021). They are used in a wide range of fields, including gaming, natural language processing, expert systems, and even creative pursuits like art and music (Paesano, 2023; Gilbert, 2021). On the more speculative side, the idea of Artificial General Intelligence (AGI) suggests that a machine could eventually solve any intellectual challenge a human can face (Younis, Sundarakani & Alsharairi, 2022; Gilbert, 2018). However, this concept remains largely theoretical; while some AI models can mimic certain aspects of human reasoning, no single system has yet achieved robust performance across all domains (Khan, Pasha & Masud, 2021; Gilbert & Gilbert, 2025c). Instead, the most effective AI systems today are designed to excel in specific, well-defined areas.

6.2. Artificial Intelligence (AI)

This section breaks down the fundamental terms and ideas central to our work. The goal is twofold: first, to clarify the complex concepts underlying the challenges and tasks we address; and second, to eliminate common misunderstandings surrounding these topics. Here, we define key concepts such as artificial intelligence itself, the notion of problem space in

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

cybersecurity, the behaviors of cyber threat actors, and the concept of cyber ranges.

VII. Artificial Intelligence in Cybersecurity

Once regarded merely as a final fallback in defense, AI-based systems have now evolved into proactive cybersecurity sentinels that outstrip traditional detection methods (Jaakkola, 2023). In the past, cybersecurity strategies largely depended on formulating, storing, and updating fixed rules to counteract cyber-attacks (Fila & Wideł, 2020; Gilbert & Gilbert, 2024w). However, this approach often lagged behind the pace at which new threats emerged—human analysts simply couldn't build or verify barriers quickly enough.

Today, leveraging historical evidence from hacker activities, AI systems develop heuristic models that anticipate future attacks (Nespoli et al., 2017). This iterative, "learn from our mistakes" method trains algorithms to detect the unique footprints attackers leave behind when deviating from normal network operations. Such adaptive learning enables these systems to recognize subtle signs of malicious intent far more efficiently than static rule-based defenses (Li & Liu, 2021).

In essence, artificial intelligence the discipline of crafting systems capable of human-like reasoning, learning, and problem-solving has become indispensable in modern cybersecurity (Jaboob, Durrah & Chakir, 2024). Given that the current defense landscape is overwhelmed by a deluge of security alerts, many incidents go unanalyzed, resulting in prolonged dwell times. Meanwhile, systems constrained by fixed human-generated rules are increasingly outpaced by the escalating sophistication of cyber threats (Joshi et al., 2025). AI-powered solutions, by integrating real-time analytics with a measure of human intuition, offer a dynamic and robust defense against these ever-evolving challenges.

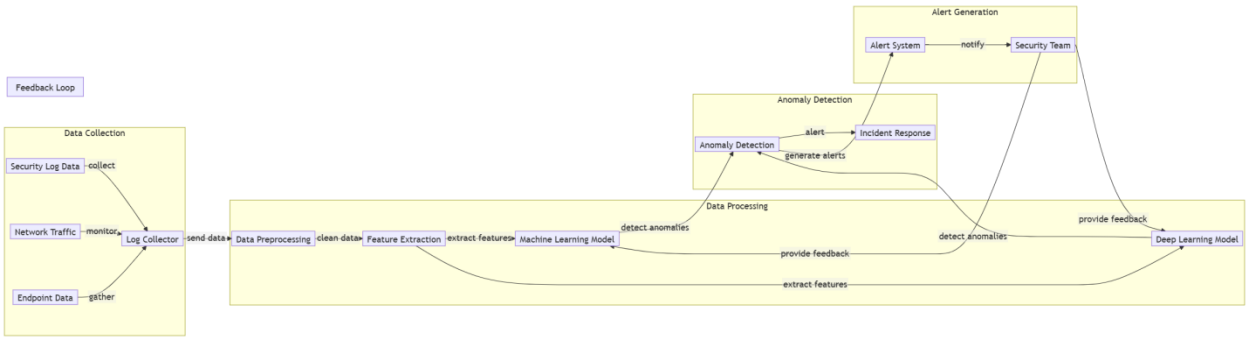

Figure 5: A cybersecurity feedback loop, showing how data is collected, processed, analyzed, and used to generate alerts for security teams.

This diagram outlines a cybersecurity feedback loop where data is continuously collected, processed, analyzed, and used to generate security alerts. It starts with data collection, where security logs, network traffic, and endpoint data are monitored and sent through a log collector. The data is then cleaned and processed, with key features extracted for analysis. A machine learning model scans for anomalies, triggering the anomaly detection system if suspicious activity is found. This leads to incident response, where security teams are alerted through an alert system. A deep learning model continuously refines the detection process by analyzing feedback, ensuring the system evolves to identify threats more accurately and reduce false alarms over time. This feedback loop enables real-time, AI-driven cybersecurity monitoring that becomes more effective with each cycle.

7.1. Machine Learning and Deep Learning Algorithms in Detection

Mardikoraem (2024), Spinner (2024) and Cheng et al. (2024) leveraged machine learning techniques to analyze malware by employing a binary classifier that yields robust evidence for evaluating specific applications Their study, which compared three widely used detection tools, found that the use of machine learning may lead to elevated false positive and false discovery rates in two of the tools; consequently, they advocate for tailored adaptations to enhance detection performance. In a related effort, Bhayo et al. (2023), introduced a multi-stage binary analysis framework that integrates machine learning. Their method involves collecting data across various stages to capture a comprehensive spectrum of malicious behaviors, which is then fed into a classifier. Experimental results from their approach reveal an improved detection capability coupled with a reduction in false positives.

The growing popularity of machine learning and deep learning for malware detection and classification stems from the limitations of traditional automated tools, such as antivirus programs and signature-based systems, which often struggle with scalability (Singh & Singh, 2021). For instance, researchers proposed a method that fuses both static and dynamic features including system calls and assembly functions into a support vector machine model (Vijayalakshmi & Jayakumar, 2024; Bitmead, 2016). Their experiments indicate that this model not only achieves a higher detection ratio but also maintains a low rate of false positives. Similarly, Kim et al. (2018), introduced a deep learning model that utilizes features extracted from the two-dimensional visualization of behavioral traces. Their model effectively distinguishes between normal benign behavior, benign setups that mimic malware, and actual malware. Validation against publicly available malware samples confirmed that the model delivers high detection accuracy while keeping false positives to a minimum (Ezenkwu & Starkey, 2019).

Enhancing Threat Detection

Contemporary artificial intelligence algorithms have significantly advanced threat detection capabilities for both network systems and computing devices. In network systems, AI-driven threat detection primarily analyzes internet traffic data to pinpoint harmful executables and scrutinizes encrypted traffic, thereby mitigating the risk of data breaches for organizations. Conversely, the application of AI for threat detection in computing devices reveals vulnerabilities predominantly in web browsers, various applications, and email—areas often exploited by spyware programs (Rao, & Jain, 2024).

These AI systems integrate scanning across multiple layers of the communications stack, including Ethernet, IP, Application Layers, DNS, and Web Log analysis, as well as incorporating signatures from various network appliances. Central to this technological progress is the deployment of machine learning-based solutions (Gorment et al., 2023). When appropriately implemented, these solutions enable systems to predict, detect, and respond to malicious activities. They achieve this by aggregating extensive datasets and converting them into formats comprehensible to AI algorithms, which subsequently analyze the data for patterns. Leveraging these learned patterns, the machine learning models are then able to predict established threats and identify previously unknown anomalies, enhancing overall cybersecurity defenses (Redhu et al., 2024).

Enhancing Threat Detection

Contemporary artificial intelligence algorithms have significantly advanced threat detection capabilities for both network systems and computing devices (Abilimi et al., 2015; Waqas et al., 2022). In network systems, AI-driven threat detection primarily analyzes internet traffic data to pinpoint harmful executables and scrutinizes encrypted traffic, thereby mitigating the risk of data breaches for organizations (Bécue, Praça & Gama, 2021; Abilimi & Adu-Manu, 2013). Conversely, the application of AI for threat detection in computing devices reveals vulnerabilities predominantly in web browsers, various applications, and email areas often exploited by spyware programs Diana (Dini & Paolini, 2025).

These AI systems integrate scanning across multiple layers of the communications stack, including Ethernet, IP, Application Layers, DNS, and Web Log analysis, as well as incorporating signatures from various network appliances (Santos, Salam & Dahir, 2024;). Central to this technological progress is the deployment of machine learning-based solutions. When appropriately implemented, these solutions enable systems to predict, detect, and respond to malicious activities. They achieve this by aggregating extensive datasets and converting them into formats comprehensible to AI algorithms, which subsequently analyze the data for patterns (Zaman et al., 2021). Leveraging these learned patterns, the machine learning models are then able to predict established threats and identify previously unknown anomalies, enhancing overall cybersecurity defenses.

VIII. Automating Incident Response

In the privacy and security domain, particularly as defined by ISO 29100, an incident is characterized as a violation of security policies, procedures, or acceptable use guidelines (Sangaroonsilp, 2024; Abilimi et al., 2013). Such incidents frequently result in unauthorized alterations to the configuration or state of networks, systems, and data including activities like reading, copying, or modifying data without proper authorization (Arshad & Asghar, 2024). Notably, when an individual introduces unauthorized changes to enterprise resources, these modifications may themselves be recognized as incidents, given that the act of alteration can imply inherent culpability even before a detailed review is undertaken (Haufe, 2024).

ISO/IEC 27002 defines incident management as a structured process tasked with ensuring the prompt identification, reporting, mitigation, documentation, investigation, and recovery support following an incident (Perkola, 2024). In contrast, ISO 27035 has preemptively broadened this perspective by acknowledging a diverse range of incident sources and addressing them through both proactive and reactive measures (Staves, 2023).

When applying automation to incident response, it is critical to adhere to these foundational definitions (Staves et al., 2022). Once a significant incident is detected, the entire process from recognition to resolution should be regarded as incident management (Abilimi & Yeboah, 2013; CANTELLI FORTI, 2019). It is essential to remain cognizant that an incident is actively unfolding, even though the typical narrative of incident response often centers on the deployment of countermeasures (Oluwawemimo, 2024). Instead of resorting to instinctive, reactionary measures such as triggering an emergency shutdown (commonly referred to as the "Big Red Button"), incident handlers should prioritize effective incident recognition and maintain clear communication with all key stakeholders, including senior management, operational teams, the Security Operations Centre, and other pertinent groups (Maezo & Rey, 2023)

This diagram outlines the cybersecurity incident management process, showing how threats are detected, analyzed, reported, and resolved, with AI playing a key role in improving efficiency. The process starts with incident detection, where AI helps identify anomalies, generate alerts, and perform initial triage. Once a potential threat is flagged, incident analysis begins, correlating data, determining the root cause, and assessing the impact. If a security issue is confirmed, it moves to incident reporting, where reports are generated, and key stakeholders are notified. In the incident resolution phase, containment strategies are implemented to prevent the threat from spreading. A SOAR (Security Orchestration, Automation, and Response) platform automates response actions, while remediation efforts work to eliminate the threat. A final post-incident review ensures lessons are learned to improve future security responses. With AI enhancing each step—from detection to resolution—this process enables faster, more accurate threat management, helping organizations stay ahead of cyber threats.

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

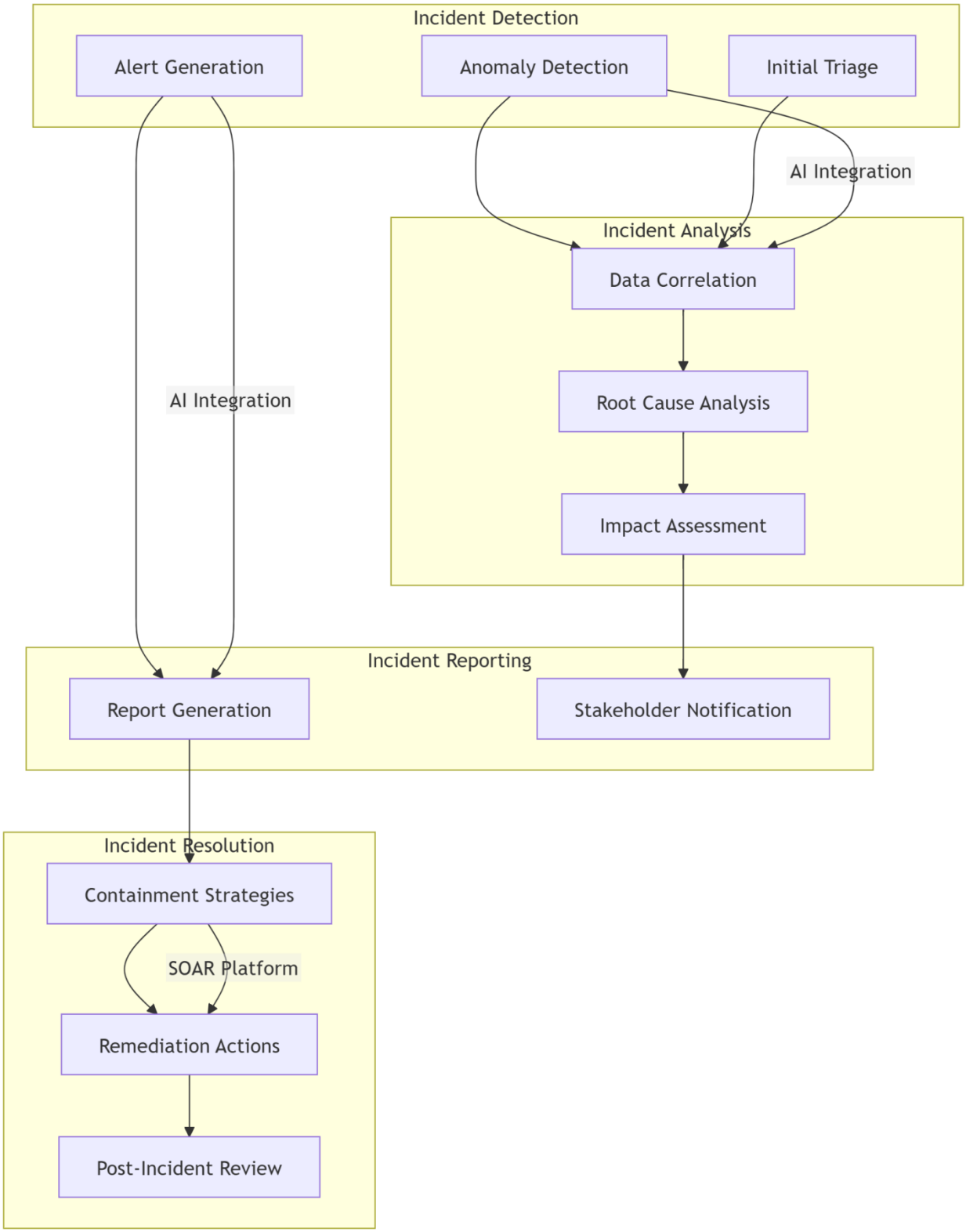

Figure 6: The cybersecurity incident management process, from detection to resolution, with AI integration enhancing key steps.

8.1. SOAR Platforms and AI Integration

Security orchestration, automation, and response (SOAR) platforms are evolving with the integration of advanced artificial intelligence; dramatically enhancing threat management processes (Yousaf & Boomsma, 2024; Kwame, Martey & Chris, 2017). These platforms now pull data from

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

diverse sources and apply contextual analysis considering factors like the attribution, intent, and deceptive tactics of threat actors to determine the most relevant response actions or gather additional data for complex investigations (Sharma & Spunda, 2025).

Machine learning plays a key role in this evolution. It not only helps guide SOAR systems in choosing the most effective course of action but also influences the relationships between various threat intelligence elements, often outperforming traditional attribution methods (Areo, 2023). As a result, security teams are better equipped to prioritize alerts and streamline investigations, boosting overall efficiency (Ismail et al., 2025).

Given that SOAR platforms are fundamentally built around the collection and analysis of threat-related information, they are poised to benefit significantly from ongoing advancements in AI (Noshi & Blaser, 2024). Projections indicate that by 2022, approximately 30% of organizations will employ machine learning to detect and respond to incidents within just 30 minutes, highlighting the importance of vendor-neutral, intelligent systems in modern security operations (Jangampet, 2024; Kinyua & Awuah, 2021).

IX. Case Studies and Applications

i. ChatOps for Cybersecurity

ChatOps in cybersecurity demonstrates how daily security operations can be executed and recorded within a central operations center using a chat-based tool (Lehmann, 2023). By incorporating chatbots into routine workflows, the system streamlines task execution through immediate data comparisons and record keeping (Ohagen et al., 2022). This approach not only provides a clear visual summary of security incidents but also enhances collaboration among security practitioners and stakeholders.

ii. Deep Learning for DDoS Mitigation

Distributed Denial of Service (DDoS) attacks are among the most destructive cyber threats, often resulting in significant downtime for online service providers and security firms (Salim, Rathore & Park, 2020). Traditional countermeasures typically lead to increased response latency or rely on specialized hardware (Gupta & Dahiya, 2021). This study introduces a reactive, software-based strategy employing deep learning techniques. Specifically, a reinforcement learning–based dynamic load balancing mechanism is developed that meets the dual requirements of low latency and effective resource management, offering a promising solution for mitigating DDoS attacks (Khalaf et al., 2019).

iii. Speech Commands Recognition

This research presents an enhanced preprocessing strategy and decoding technique for speech direction recognition (Yu et al. 2020). The proposed method utilizes overlapping frames to generate a two-channel spectrogram, preserving resolution while emphasizing inter-channel differences (Tan, Wang & Wang, 2022). This enhancement benefits CNN models employing similar architectures, especially when channel-based pooling is applied to the output (Fırat, 2024). Experimental results show that these refinements accelerate the convergence of the deep neural network, reduce overfitting, and improve overall performance for specific speech recognition tasks (Prabhavalkar et al., 2023).

iv. Image Captioning

The study of image captioning focuses on the advantages of cross-modal recognition (Zhang et al., 2023). The approach integrates a Pre-CNN network with a decoder that sequentially generates descriptive text for an image (Rath, Das & Pattanayak, 2024). Initially, the decoder produces a series of text features, which then query the cross-modal features derived from the Pre-CNN network (Thomas & Kovashka, 2019). A back encoder subsequently aggregates the visual information into two-dimensional feature maps (Wu et al., 2023). Correlations between analogous representations are computed using dual cross-modal queries to normalize the data, ultimately conditioning the decoder parameters. The model is then optimized by minimizing the loss derived from the cross-queued maximum probability (Zhang et al., 2024).

The case studies presented above illustrate a diverse range of artificial intelligence applications in cybersecurity (Lu et al., 2024). By leveraging state-of-the-art models and methodologies, these applications enhance threat detection, response strategies, speech recognition, image captioning, and overall system security (Wu et al., 2023). Each approach offers unique benefits and demonstrates significant potential for advancing cybersecurity practices across various industries.

This diagram compares different AI-driven applications and their impact on cybersecurity, threat detection, and data processing. ChatOps for Cybersecurity improves security operations by integrating chatbots, a central operations center, and visual summaries of incidents for faster responses. Deep Learning for DDoS Mitigation uses reinforcement learning and advanced preprocessing techniques to enhance attack detection while optimizing latency and resource use. Speech Command Recognition refines CNN-based detection with two-channel spectrograms and cross-modal recognition, improving accuracy. Meanwhile, Image Captioning leverages pre-CNN networks and optimized decoding for more precise image descriptions. In comparing these case studies, this analysis highlights best practices, key takeaways, and differences, helping refine AI applications to make them more efficient, adaptable, and effective in real-world scenarios.

9.1. Real-world Implementations and Success Stories

A careful examination of current artificial intelligence (AI) applications reveals valuable lessons that can be translated into various cybersecurity contexts (Das & Sandhane, 2021; Yeboah, Odabi & Abilimi Odabi, 2016). Despite the inherent differences in risk profiles and threat models across cybersecurity scenarios, there exists a notable gap between the rapid development of cutting-edge AI solutions and the level of comprehension and confidence that cybersecurity professionals have in these tools (Goswami et al., 2024). To bridge this gap, it is essential to deconstruct existing methodologies into their fundamental components and hypotheses, clarifying which elements can be modified and

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

which assumptions must be maintained for success (Charmet et al., 2022).

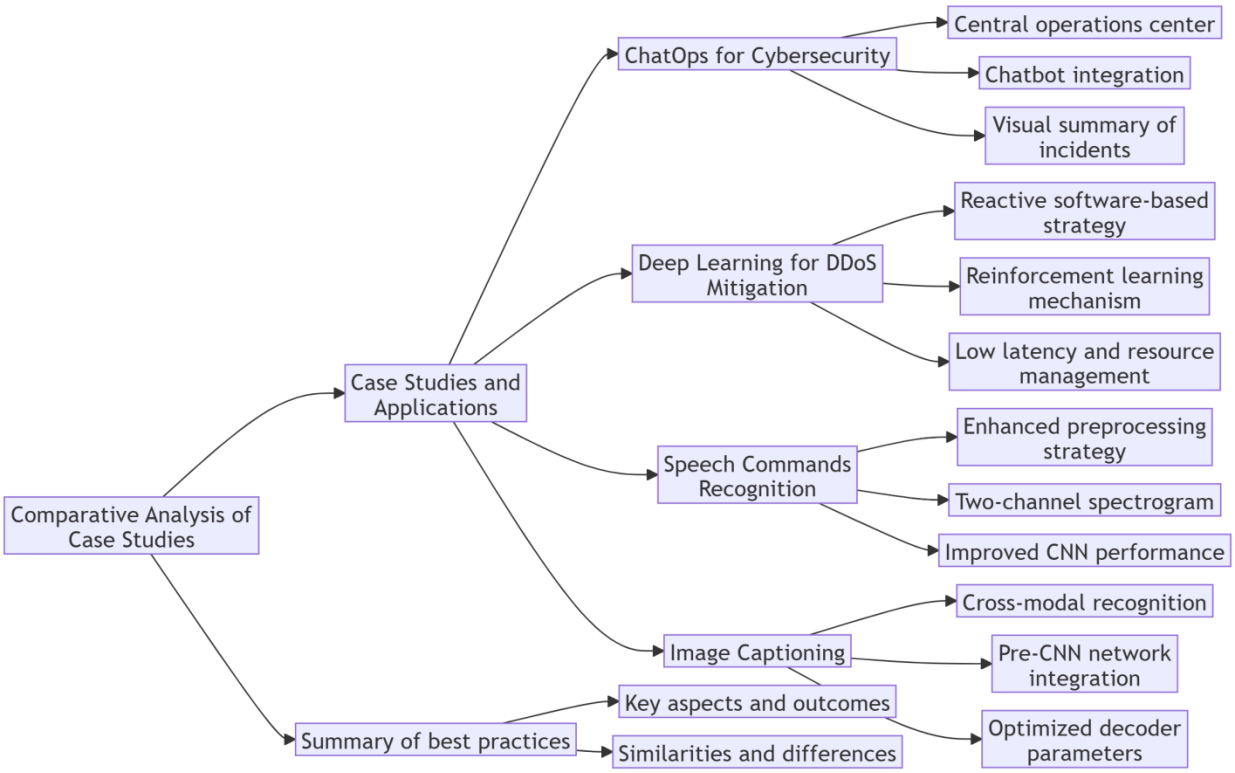

Figure 7: A comparative analysis of case studies related to AI applications.

Empirical evidence of AI's effectiveness is well-documented across diverse fields, offering a wealth of industrial best practices that include detailed guidelines, standardized procedures, and comprehensive profiles (Loaiza et al., 2022). These resources not only underscore the transformative impact of AI and deep learning techniques but also provide a framework for evaluating their potential application within cybersecurity (Capuano et al., 2022). For example, guidelines from organizations dedicated to ethical data and research, as well as collaborative initiatives like the Partnership on AI, serve to foster an environment where both public and private entities can jointly address the security challenges associated with AI technologies (Ozkan-Okay et al., 2024).

The integration of AI in cybersecurity is largely motivated by a series of success stories, particularly those involving deep learning, where these technologies have safeguarded data-intensive systems from social media networks to extensive enterprise infrastructures (Kaur, Gabrijelčič & Klobučar, 2023; Avcı, 2024). A thorough analysis of these implementations is crucial, as it enhances our qualitative understanding of the role AI can play in strengthening cybersecurity defenses. Ultimately, such insights contribute to bridging the divide between current cybersecurity challenges and the adoption of state-of-the-art AI techniques (Bechtsis et al., 2022).

X. Challenges and Ethical Considerations

This section delves into the dynamic intersection of AI and cybersecurity, outlining the key challenges faced by businesses, governments, and military organizations in the near to medium term (Prasad & Kulkarni, 2023). It reviews prominent vulnerabilities and positions our research within a broader context of AI applications in cybersecurity (Singh & Kaunert, 2025; Yeboah & Abilimi, 2013). We introduce a comprehensive classification framework that maps various research domains and benchmarks, offering insights into both the technical (code and architecture) and ethical dimensions of AI in security (Ali et al. 2024; Yeboah, Opoku-Mensah & Abilimi, 2013a). This approach not only partitions key techniques but also examines their interactions with established research areas. In addition, we summarize the main technical advancements achieved and discuss ethical considerations, future STOA MDA tasks, emerging challenges, and concluding insights.

The growth in internet-connected devices and the expanding network edges have amplified potential entry points for cyber threats (Djenna, Harous & Saidouni, 2021). Each connected device represents a possible target for malicious actors, especially as these systems become integral to large-scale corporate and governmental infrastructures. Technologically, AI builds on an extensive toolkit that promises significant business and labor transformations in the coming years (Mallick & Nath, 2024; Yeboah, Opoku-Mensah

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

& Abilimi, 2013b). However, the ethical, legal, and social challenges associated with these advances remain in early development. Society often embraces new technologies more rapidly than their regulatory and ethical frameworks can adapt. Efforts are underway to integrate these challenges into policies and MDA standards, ensuring that the deployment of AI in security—and other fields—addresses its broad and disruptive impacts.

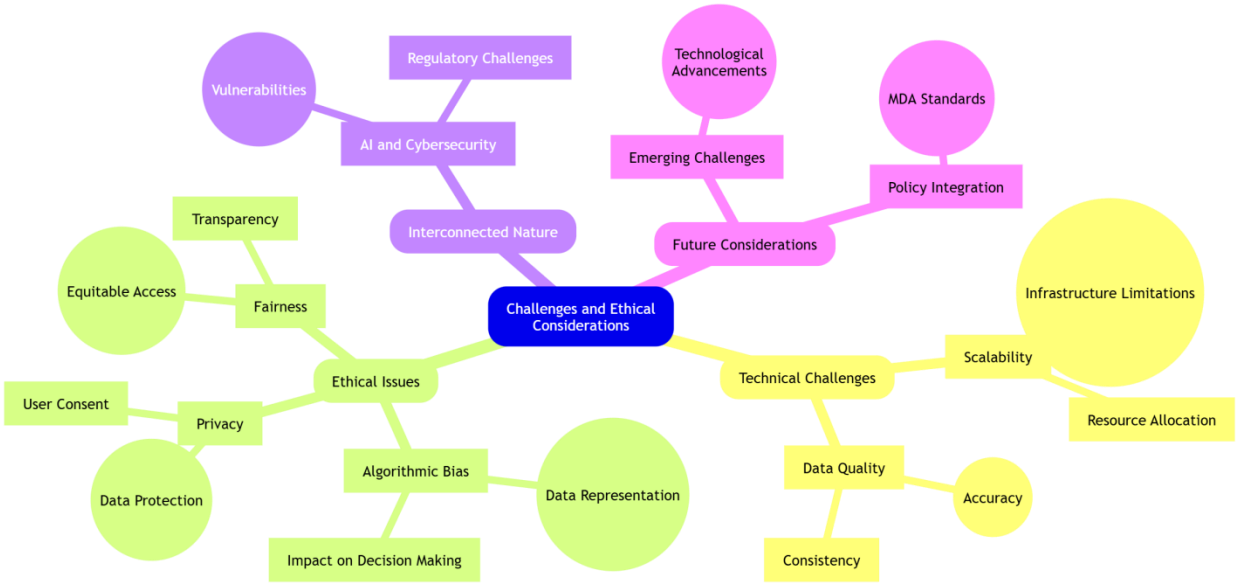

Figure 8: The challenges and ethical considerations in AI and cybersecurity.

This diagram highlights the key ethical, technical, and security challenges in AI and cybersecurity, along with future considerations. Ethical concerns focus on fairness, transparency, and privacy, ensuring AI systems avoid bias and protect user data. Technical challenges include scalability, resource allocation, and maintaining data quality, all essential for reliable AI decision-making. As AI becomes more integrated into cybersecurity, new vulnerabilities and regulatory challenges emerge, requiring constant updates to security frameworks. Looking ahead, the focus must be on policy integration, standardization, and proactive governance to ensure AI evolves responsibly while staying secure. Balancing innovation, security, and ethics will be key to AI's success in the future.

10.1 Bias and Fairness in AI Algorithms

As AI and machine learning increasingly influence areas like safety and privacy, developers in cybersecurity must critically assess the broader impacts of the technologies they build (Abdulhussein, 2024; Opoku-Mensah, Abilimi & Boateng, 2013). AI has become integral to decision-making systems that underpin the efficiency and security of the internet, prompting a global conversation about ethical AI (Jimmy, 2021). In cybersecurity, ensuring fairness in algorithmic processes particularly through fair transfer learning between supervised and unsupervised settings is emerging as a critical issue.

The rapid advancements in computing power and the abundance of big data have led to more sophisticated AI algorithms, which, while beneficial, also raise concerns regarding fairness and reliability (Akhtar & Rawol, 2024; Opoku-Mensah, Abilimi & Amoako, 2013). As algorithmic decision-making becomes ubiquitous across various high-impact sectors, it highlights the need to address ethical issues at every level (Du & Xie, 2021). This is particularly crucial in cybersecurity, where the reliance on these systems can widen existing inequalities. Addressing fairness is not only a regulatory imperative but also a business necessity, as companies that successfully integrate AI must also tackle these ethical challenges to enhance their operational capabilities (Rezaei, Pironti & Quaglia, 2024). In this light, independent research and investment in skill development are essential to resolving the pressing issues at the nexus of AI and cybersecurity.

TABLE 1: Bias and Fairness in AI Algorithms

Category	Key Insights
AI's Role in Cybersecurity	AI and machine learning are crucial for decision-making, efficiency, and security in cybersecurity systems.
Ethical AI Concerns	Ensuring fairness in AI-driven cybersecurity processes, especially in transfer learning between supervised and unsupervised models, is a growing challenge.
Advancements vs. Risks	While big data and computing power have improved AI sophistication, they also raise concerns about fairness, reliability, and bias.
High-Impact Sectors	AI-based decisions influence critical industries, including cybersecurity, and can widen inequalities if fairness is overlooked.
Regulatory & Business Needs	Addressing bias in AI is both a legal requirement and a business necessity, as fairness strengthens operational capabilities.
Path to Solutions	Independent research and investment in AI skill development are vital to resolving ethical and fairness concerns in cybersecurity AI.

This table simplifies the core ideas, making it easier to grasp the challenges and necessary actions for ensuring fairness in AI-driven cybersecurity.

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

10.2. Emerging Technologies in AI and Cybersecurity

Our analysis categorizes AI's true functionality as being supported by internet signals and their interplay within cyber threat environments (Khalaf et al., 2019). The first step is defining key indicators that clarify how AI and cybersecurity relate. Technically, AI provides advanced warning signals about rising cyber threats from data theft to both human and automated risks (De Azambuja et al., 2023). It also shapes the extent to which cybersecurity systems can manage increased dangers.

After thorough evaluation, these emerging AI trends can be synthesized into a comprehensive model for Cyber Threat Internet Security, which will help determine both its limitations and the nuances of patent applications in the field (Kaur, Gabrijelčič & Klobučar, 2023). A subsequent investigation is needed to pinpoint vulnerabilities and limitations in AI-powered cybersecurity, both practically and conceptually. Unlike early studies, a modern conceptual model may also need to address challenges like insufficient AI literacy and gaps in gender-sensitive security updates (Arisdakessian et al., 2022).

TABLE 2: Emerging Technologies in AI and Cybersecurity.

Category	Key Insights
AI's Role in Cybersecurity	AI relies on internet signals and cyber threat environments to provide advanced warning signals for cyber threats. It helps manage risks from both human and automated attacks.
Comprehensive Cyber Threat Model	AI trends are being synthesized into a Cyber Threat Internet Security model to identify limitations and patent-related nuances. Further research is needed to pinpoint AI vulnerabilities in cybersecurity.
Challenges in AI-Powered Security	Unlike traditional machine learning models (which analyze physical features like images or voices), cybersecurity data is complex. Issues like insufficient AI literacy and gender-sensitive security gaps need attention.
Regulatory & Geopolitical Concerns	Automating cybersecurity responses requires careful handling of regulatory and privacy concerns. A key question is how AI should quantify its response to threats while balancing user privacy.
AI as a Predictive Tool	AI can detect patterns and forecast risks, guiding cybersecurity strategies. As Frank Mercer puts it, AI helps navigate potential threats like a bus driver avoids traffic jams.
AI's Growing Impact	AI integration in cybersecurity is expanding, with initial trials leading to automation. Companies like IBM are forming partnerships to address cyber threats and talent shortages.
Biggest Opportunity: Behavioral Research	AI can analyze normal vs. abnormal behavior, flagging anomalies in real-time. Similar to behavioral biometric monitoring, this allows systems to instantly adjust and prevent unauthorized access.

This table highlights how AI is reshaping cybersecurity, identifying threats in real-time, automating security measures, and improving risk forecasting while tackling ethical, regulatory, and technical challenges.

Research in this area is fundamental for integrating AI into cybersecurity. One of the major challenges is identifying the right functions for AI in this space (Attkan & Ranga, 2022). Unlike machine learning models that use physical features for tasks like image or voice recognition, cybersecurity data is far more complex and less straightforward. Addressing geopolitical and regulatory issues in cybersecurity is crucial to automate protection effectively (Moustafa et al., 2023). For example, if an operating system flags a potential threat, how should an AI model quantify its response? And how can we balance privacy concerns while imitating real user behavior?

As Frank Mercer, USA Cyberpreneur SBA State Director, puts it, "AI can look for patterns and forecast. It acts like a guide, helping navigate through potential blockages or threats; much like a bus driver is advised on the best routes to avoid traffic jams." Currently, the integration of AI into cybersecurity is progressing steadily, with initial trials paving the way for more automated systems (Zaman et al., 2021; World Health Organization, 2023).

The role of AI in cybersecurity is growing, and partnerships with experts, such as those at IBM, offer exciting prospects amid the rising demand for cyber safety and the ongoing talent shortage (Bécue, Praça & Gama, 2021; Samson & Sumi, 2019). One of the biggest opportunities for AI lies in behavioral researchenabling systems to understand what constitutes normal behavior and quickly flag anomalies (Waqas et al., 2022). This approach, similar to behavioral biometric monitoring, allows systems to adjust their settings immediately when they detect potential threats, effectively stopping unauthorized access by learning what typical behavior is (Radanliev et al., 2021).

XI. Findings, Conclusions, Recommendations, and Future Trends

The summary of the key findings, conclusions, recommendations, and future trends from the research article:

Key Findings

- Enhanced Threat Detection and Rapid Response: AI-driven systems have proven capable of ingesting, analyzing, and correlating vast streams of security data far more efficiently than traditional, rule-based approaches. This result in faster detection of anomalies, reduced false positives, and accelerated incident response times.
- Augmentation, Not Replacement: Rather than replacing human analysts, AI acts as a co-helper within Security Operations Centers (SOCs). It supports security personnel by flagging subtle patterns and abnormal behaviors that might otherwise be overlooked during manual analysis.
- Real-World Efficacy: Case studies—including implementations for ChatOps, deep learning-based DDoS mitigation, speech command recognition, and image captioning—demonstrate that AI can be successfully applied across various cybersecurity functions. These examples highlight how AI contributes to improved operational efficiency and stronger defense mechanisms.
- Challenges and Ethical Considerations: Despite its advantages, the integration of AI in cybersecurity is not without hurdles. Technical challenges such as scalability and data quality, along with ethical concerns like algorithmic bias, privacy, and fairness, require careful management.

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

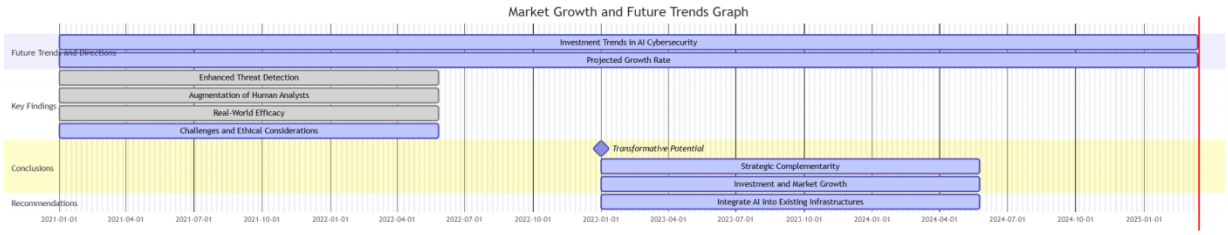

Figure 9: The market growth trends and future projections in AI-driven cybersecurity.

This graph highlights the growing role of AI in cybersecurity, showing increasing investment trends and future projections. AI is expected to enhance threat detection, support human analysts, and improve real-world security, but ethical challenges must be addressed. As investment in AI-driven security continues to rise, its transformational potential becomes clear—working alongside human experts rather than replacing them. The key recommendation is to ensure AI is seamlessly integrated into existing cybersecurity infrastructures, balancing technological advancements with ethical considerations for a more effective and secure future.

XII. Conclusions

- Transformative Potential: The research confirms that artificial intelligence represents a transformative force in cybersecurity. By enabling real-time analytics and proactive threat detection, AI addresses the shortcomings of legacy systems and adapts to the rapidly evolving threat landscape.
- Strategic Complementarity: AI enhances traditional cybersecurity measures by reducing the workload on human analysts and mitigating risks associated with manual processes. However, its effectiveness depends on a balanced integration with existing SOC processes, ensuring that human judgment complements automated decision-making.
- Investment and Market Growth: The growing investment in AI-enhanced cybersecurity as evidenced by multi-billion dollar figures—reflects a market trend toward adopting more sophisticated, data-driven defense strategies. This trend underscores the necessity of embedding AI within modern cybersecurity frameworks to safeguard digital assets.

Recommendations

- Integrate AI into Existing Infrastructures: Organizations should work toward embedding AI into their current SOC operations. This integration should be incremental, ensuring that AI systems complement human expertise without overwhelming established workflows.
- Adopt Best Practices from Case Studies: Leveraging insights from successful implementations (for example; ChatOps, dynamic load balancing for DDoS, and multimodal data analysis) can guide the development of tailored AI strategies. Organizations are encouraged to study these real-world examples to adopt practices that match their unique security needs.
- Address Technical and Ethical Challenges: It is critical to implement measures that tackle technical issues such as scalability and integration challenges, while also establishing frameworks to manage ethical concerns. This includes ongoing training for staff, regular audits of AI systems for bias, and ensuring that privacy and data protection remain at the forefront.
- Foster Collaboration and Innovation: Encouraging partnerships between industry experts, academic researchers, and cybersecurity professionals can facilitate knowledge sharing. Such collaborations can drive further innovation and help in developing robust frameworks that harness AI's full potential.

Future Trends

- Emerging AI Techniques: Future research is likely to explore advanced models such as Bayesian deep learning, recurrent neural networks (RNNs), and long short-term memory (LSTM) networks. These techniques are expected to enhance the capability of AI systems to deal with sequential data and uncertainty, which is critical in real-time threat detection.
- Integration of Natural Language Processing (NLP): NLP is emerging as an important tool in cybersecurity for analyzing textual data—from threat reports to real-time alerts. Improved NLP algorithms can further aid in understanding and mitigating cyber threats by processing and interpreting large volumes of unstructured data.
- Focus on Fairness and Privacy: As AI systems become more prevalent, future developments will need to focus on ensuring these systems are fair, unbiased, and respectful of user privacy. Research into mitigating bias and enhancing transparency in AI algorithms is expected to be a major focus.
- Robust Risk Assessment and Adaptive Security Models: There is growing interest in integrating AI into risk assessment processes to evaluate potential vulnerabilities in cybersecurity architectures. Future systems may rely on adaptive security models that continuously learn and evolve to counter emerging threats, shifting away from static defense mechanisms.
- Increased Industry Collaboration: With ongoing talent shortages and rapid technological advancements, collaborative efforts between private enterprises, government bodies, and academic institutions will likely become more common. Such partnerships will help standardize AI applications in cybersecurity and drive the next generation of defense technologies.

Chris Gilbert, Mercy Abiola Gilbert, Maxwell Dorgbefu Jnr, Duah Jeremiah Leakpor, Kwitee D. Gaylah, and Isaac A. Adetunde, "Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 87-104, 2025.

REFERENCE

1. Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D. E. A., ... & Prokop, L. (2024). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *Results in Engineering, 102647*.
2. Abdulhussein, M. (2024). The impact of artificial intelligence and machine learning on organizations cybersecurity. *Liberty University*.
3. Abilimi,C.A, Asante,M, Opoku-Mensah, E & Boateng, F.O. (2015). Testing for Randomness in Pseudo Random Number Generators Algorithms in a Cryptographic Application.Computer Engineering and Intelligent Systems, www.iiste.org, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.9, 2015
4. Abilimi, C. A., & Adu-Manu, K. S. (2013). *Examining the impact of Information and Communication Technology capacity building in High School education in Ghana*. International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 9, September - 2013
5. Abilimi, C.A., Amoako, L., Ayembillah, J. N., Yeboah, T.(2013). Assessing the Availability of Information and Communication Technologies in Teaching and Learning in High School Education in Ghana. *International Journal of Engineering Research and Technology, 2(11), 50 - 59*.
6. Abilimi, C. A. & Yeboah, T. (2013). Assessing the challenges of Information and Communication Technology in educational development in High Schools in Ghana. International Journal of Engineering Research & Technology (IJERT).ISSN: 2278-0181, Vol. 2 Issue 11, November - 2013
7. Akhtar, Z. B., & Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. *IT Journal Research and Development, 9(1), 50-67*.
8. AL-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and Systems, 55(2), 302-330*.
9. Ali, G., Mijwil, M. M., Buruga, B. A., Abotaleb, M., & Adamopoulos, I. (2024). A survey on artificial intelligence in cybersecurity for smart agriculture: State-of-the-art, cyber threats, artificial intelligence applications, and ethical concerns. *Mesopotamian Journal of Computer Science, 2024*, 53-103.
10. Alsamhi, S. H., Kumar, S., Hawbani, A., Shvetsov, A. V., Zhao, L., & Guizani, M. (2024). Synergy of human-centered AI and cyber-physical-social systems for enhanced cognitive situation awareness: applications, challenges and opportunities. *Cognitive Computation, 16(5), 2735-2755*.
11. Arisdakessian, S., Wahab, O. A., Mourad, A., Otrok, H., & Guizani, M. (2022). A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions. *IEEE Internet of Things Journal, 10(5), 4059-4092*.
12. Areo, G. (2023). Advancing Cyber Resilience through the Convergence of SIEM, SOAR, and AI Technologies.
13. Arshad, R., & Asghar, M. R. (2024). Characterisation and quantification of user privacy: key challenges, regulations, and future directions. *IEEE Communications Surveys & Tutorials*.
14. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12(6), 1333*.
15. Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems, 8(4), 3559-3591*.
16. Avcı, C. (2024). Cybersecurity design of data-intensive systems (Doctoral dissertation, Wageningen University and Research).
17. Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review, 54(5), 3849-3886*.
18. Bechtsis, D., Tsolakis, N., Iakovou, E., & Vlachos, D. (2022). Data-driven secure, resilient and sustainable supply chains: gaps, opportunities, and a new generalised data sharing and data monetisation framework. *International Journal of Production Research, 60(14), 4397-4417*.
19. Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Engineering Applications of Artificial Intelligence, 123, 106432*.
20. Bhardwaj, A. (2024). Insecure digital frontiers: Navigating the global cybersecurity landscape. *CRC Press*.
21. Bitmead, R. (2016). Our Robots, Ourselves: Robotics and the Myths of Autonomy [Bookshelf]. *IEEE Control Systems Magazine, 36(6), 99-102*.
22. CANTELLI FORTI, A. (2019). Mitigation and Incident Management methodologies for Critical Infrastructure protection.
23. Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access, 10, 93575-93600*.
24. Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In *Artificial intelligence for societal issues* (pp. 3-25). Cham: *Springer International Publishing*.
25. Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., Gimenez, P. F., Han, Y., Jmila, H., ... & Zhang, Z. (2022). Explainable artificial intelligence for cybersecurity: a literature survey. *Annals of Telecommunications, 77(11), 789-812*.
26. Cheng, X., Chen, B., Li, P., Gong, J., Tang, J., & Song, L. (2024). Training compute-optimal protein language models. *Advances in Neural Information Processing Systems, 37, 69386-69418*.
27. Christopher, A. A.(2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm.International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 8, August - 2013.
28. Cofer, D., Amundson, I., Babar, J., Hardin, D., Slind, K., Alexander, P., ... & Shackleton, J. (2022). Cyberassured systems engineering at scale. *IEEE Security & Privacy, 20(3), 52-64*.
29. Das, R., & Sandhane, R. (2021, July). Artificial intelligence in cyber security. In *Journal of Physics: Conference Series (Vol. 1964, No. 4, p. 042072). IOP Publishing*.
30. De Azambuja, A. J. G., 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*.
31. Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing.
32. Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. *Computers, 14(3), 87*.
33. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences, 11(10), 4580*.
34. Du, S., & Xie, C. (2021). Paradoxes of artificial intelligence in consumer markets: Ethical challenges and opportunities. *Journal of Business Research, 129, 961-974*.
35. Edmund, E., & Enemosah, A. (2024). AI and machine learning in cybersecurity: Leveraging AI to predict, detect, and respond to threats more efficiently.
36. Ezenkwu, C. P., & Starkey, A. (2019). Machine autonomy: Definition, approaches, challenges and research gaps. In *Intelligent Computing: Proceedings of the 2019 Computing Conference, Volume 1* (pp. 335-358). *Springer International Publishing*.
37. Fila, B., & Wideł, W. (2020, June). Exploiting attack–defense trees to find an optimal set of countermeasures. In *2020 IEEE 33rd computer security foundations symposium (CSF)* (pp. 395-410). *IEEE*.
38. Fırat, H. (2024). Classification of microscopic peripheral blood cell images using multibranch lightweight CNN-based model. *Neural Computing and Applications, 36(4), 1599-1620*.
39. Gilbert, C.(2012). The Quest Of Father And Son: Illuminating Character Identity, Motivation, And Conflict In Cormac Mccarthy's The Road. English Journal, Volume 102, Issue Characters And Character, P. 40 - 47. Https://Doi.Org/10.58680/Ej201220821.
40. Gilbert, C. (2018). Creating Educational Destruction: A Critical Exploration Of Central Neoliberal Concepts And Their Transformative Effects On Public Education. The Educational Forum, 83(1), 60–74. Https://Doi.Org/10.1080/00131725.2018.1505017.

41. Gilbert, C. (2021). Walking The Popular Education Spiral - An Account And Analysis Of Participatory Action Research With Teacher Activists. Educational Action Research, 30(5), 881–901. Https://Doi.Org/10.1080/09650792.2021.1875856
42. Gilbert, C. (2022). Making The Invisible Visible: Professional Development To Support Teacher Activism. Kappa Delta Pi Record, 58(1), 14–19. Https://Doi.Org/10.1080/00228958.2022.2005426
43. Gilbert, C. & Gilbert, M.A.(2024a). Unraveling Blockchain Technology: A Comprehensive Conceptual Review. International Journal Of Emerging Technologies And Innovative Research (Www.Jetir.Org | Ugc And Issn Approved), Issn:2349-5162, Vol.11, Issue 9, Page No. Ppa575-A584, September-2024, Available At : Http://Www.Jetir.Org/Papers/Jetir2409066.Pdf
44. Gilbert, C. & Gilbert, M.A.(2024b). Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. International Journal of Latest Technology in Engineering Management & Applied Science, 13(8), 132-141. https://doi.org/10.51583/IJLTEMAS.2024.130816
45. Gilbert, C. & Gilbert, M.A.(2024c). The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges.Global Scientific Journals.ISSN 2320-9186,12(9),427-441. https://www.globalscientificjournal.com/researchpaper/The_Impact_of_AI_on_Cybersecurity_Defense_Mechanisms_Future_Trends_and_Challenges_.pdf.
46. Gilbert, C. & Gilbert, M.A. (2024d). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. *International Journal of Scientific Research and Modern Technology*, *3*(9), 9-9.
47. Gilbert, C. & Gilbert, M.A.(2024e). Transforming Blockchain: Innovative Consensus Algorithms for Improved Scalability and Security. International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 10, page no.b299-b313, October-2024, Available :http://www.jetir.org/papers/JETIR2410134.pdf
48. Gilbert, C. & Gilbert, M.A. (2024f). Future Privacy Challenges: Predicting the Agenda of Webmasters Regarding Cookie Management and Its Implications for User Privacy. International Journal of Advanced Engineering Research and Science, ISSN (Online): 2455-9024,Volume 9, Issue 4, pp. 95-106.
49. Gilbert, C., & Gilbert, M. A. (2024g). Navigating the Dual Nature of Deepfakes: Ethical, Legal, and Technological Perspectives on Generative Artificial Intelligence (AI) Technology. *International Journal of Scientific Research and Modern Technology*, *3*(10). https://doi.org/10.38124/ijsrmt.v3i10.54
50. Gilbert, C., & Gilbert, M. A. (2024h). Revolutionizing Computer Science Education: Integrating Blockchain for Enhanced Learning and Future Readiness. International Journal of Latest Technology in Engineering, Management & Applied Science, ISSN 2278-2540, Volume 13, Issue 9, pp.161-173.
51. Gilbert, C. & Gilbert, M.A. (2024i). Unlocking Privacy in Blockchain: Exploring Zero-Knowledge Proofs and Secure Multi-Party Computation Techniques. Global Scientific Journal (ISSN 2320-9186) 12 (10), 1368-1392.
52. Gilbert, C. & Gilbert, M.A. (2024j). The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation.International Research Journal of Advanced Engineering and Science (ISSN: 2455-9024), Volume 9, Issue 4, pp. 170-181.
53. Gilbert, C. & Gilbert, M.A.(2024k). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 219-236.
54. Gilbert, C., & Gilbert, M. A. (2024l). The security implications of artificial intelligence (AI)-powered autonomous weapons: Policy recommendations for international regulation. *International Research Journal of Advanced Engineering and Science*, *9*(4), 205–219.
55. Gilbert, C., & Gilbert, M. A. (2024m). The role of quantum cryptography in enhancing cybersecurity. *International Journal of Research Publication and Reviews*, *5*(11), 889–907. https://www.ijrpr.com
56. Gilbert, C., & Gilbert, M. A. (2024n). Bridging the gap: Evaluating Liberia's cybercrime legislation against international standards. *International Journal of Research and Innovation in Applied Science (IJRIAS)*, *9*(10), 131–137. https://doi.org/10.51584/IJRIAS.2024.910013
57. Gilbert, C., & Gilbert, M. A. (2024o). The Effectiveness of Homomorphic Encryption in Protecting Data Privacy. *International Journal of Research Publication and Reviews*, *5*(11), 3235-3256. https://www.ijrpr.com.
58. Gilbert, C., & Gilbert, M. A. (2024p). Cryptographic Foundations And Cybersecurity Implications Of Blockchain Technology. *Global Scientific Journals*, ISSN 2320-9186,12(11),464-487. https://www.globalscientificjournal.com
59. Gilbert, C., & Gilbert, M. A. (2024q). Advancing privacy standards through education: The role of academic initiatives in enhancing privacy within Cardano's blockchain ecosystem. *International Research Journal of Advanced Engineering and Science*, *9*(4), 238–251.
60. Gilbert, C., & Gilbert, M. A. (2024r). Leveraging artificial intelligence (AI) by a strategic defense against deepfakes and digital misinformation. *International Journal of Scientific Research and Modern Technology*, *3*(11). https://doi.org/10.38124/ijsrmt.v3i11.76
61. Gilbert, C., & Gilbert, M. A. (2024s). Evaluation of the efficiency of advanced number generators in cryptographic systems using a comparative approach. *International Journal of Scientific Research and Modern Technology*, *3*(11). https://doi.org/10.38124/ijsrmt.v3i11.77
62. Gilbert, C., & Gilbert, M. A. (2024t). Cybersecurity risk management frameworks for critical infrastructure protection. *International Journal of Research Publication and Reviews*, *5*(12), 507–533. https://www.ijrpr.com/
63. Gilbert, C., & Gilbert, M. A. (2024u). Organizational and leadership aspects of cybersecurity governance. *International Journal of Research Publication and Reviews*, *5*(12), 1174–1191. Retrieved from www.ijrpr.com
64. Gilbert, C., & Gilbert, M. A. (2024v). The development and evolution of cryptographic algorithms in response to cyber threats. *International Journal of Research Publication and Reviews*, *5*(12), 1149–1173. Retrieved from www.ijrpr.com
65. Gilbert, C., & Gilbert, M. A. (2024w). Privacy-preserving data mining and analytics in big data environments. *Global Scientific Journal*, *12*(12). Retrieved from www.globalscientificjournal.com
66. Gilbert, C., & Gilbert, M. A. (2024x). Investigating the challenges and solutions in cybersecurity using quantum computing and cryptography. International Research Journal of Advanced Engineering and Science, 9(4), 291–315.
67. Gilbert, C., & Gilbert, M. A. (2024y). The integration of blockchain technology into database management systems for enhanced security and transparency. International Research Journal of Advanced Engineering and Science, 9(4), 316–334.
68. Gilbert, C., & Gilbert, M. A. (2025a). *Artificial intelligence (AI) and machine learning (ML) for predictive cyber threat intelligence (CTI)*. International Journal of Research Publication and Reviews, 6(3), 584–617. http://www.ijrpr.com
69. Gilbert, C., & Gilbert, M. A. (2025b). Continuous user authentication on mobile devices. International Research Journal of Advanced Engineering and Science, 10(1), 158–173.
70. Gilbert, C., & Gilbert, M. A. (2025c). Patterns and vulnerabilities of cryptocurrency-related cybercrimes. Global Scientific Journal, 13(3), 1950-1981. *https://www.globalscientificjournal.com*
71. Gilbert, M.A., Oluwatosin, S. A., & Gilbert, C.(2024). An investigation into the types of role-based relationships that exist between lecturers and students in universities across southwestern nigeria: a sociocultural and institutional analysis. Global Scientific Journal, ISSN 2320-9186, Volume 12, Issue 10, pp. 263-280.
72. Gilbert, M.A., Auodo, A. & Gilbert, C.(2024). Analyzing Occupational Stress in Academic Personnel through the Framework of Maslow's Hierarchy of Needs. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 620-630.
73. Gorment, N. Z., Selamat, A., Cheng, L. K., & Krejcar, O. (2023). Machine learning algorithm for malware detection: Taxonomy, current challenges, and future directions. *IEEE Access, 11, 141045-141089*.
74. Goswami, S. S., Mondal, S., Halder, R., Nayak, J., & Sil, A. (2024). Exploring the impact of artificial intelligence integration on cybersecurity: A comprehensive analysis. *Journal of Industrial Intelligence, 2(2), 73-93*.

75. Gupta, B. B., & Dahiya, A. (2021). Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures. *CRC Press*.
76. Haufe, K. (2024, February). Information Privacy Management—A Process Reference Model. In *International Conference on Theoretical and Applied Computing* (pp. 129-141). *Singapore: Springer Nature Singapore*.
77. Hopgood, A. A. (2021). Intelligent systems for engineers and scientists: a practical guide to artificial intelligence. *CRC Press*.
78. Ismail, I., Kurnia, R., Brata, Z. A., Nelistiani, G. A., Heo, S., Kim, H., & Kim, H. (2025). Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic AI.
79. Jaboob, A., Durrah, O., & Chakir, A. (2024). Artificial intelligence: An overview. *Engineering Applications of Artificial Intelligence, 3-22*.
80. Jaakkola, M. (2023). Reporting on artificial intelligence: A handbook for journalism educators.
81. Jangampet, V. D. (2024). CYBERSECURITY EVOLUTION MODEL: AI/ML IN SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE. *International Journal of Computer Engineering and Technology (IJCET), 15(1), 1-6*.
82. Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library, 1, 564-74*.
83. Jimmy, F. N. U. (2024). Cyber security vulnerabilities and remediation through cloud security tools. *Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023, 2(1), 129-171*.
84. Joshi, R., Pandey, K., Kumari, S., & Badola, R. (2025). Artificial Intelligence: A Gateway. *The Intersection of 6G, AI/Machine Learning, and Embedded Systems: Pioneering Intelligent Wireless Technologies*, 146.
85. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97, 101804*.
86. Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. *IEEE Access, 7, 51691-51713*.
87. Khan, F. H., Pasha, M. A., & Masud, S. (2021). Advancements in microprocessor architecture for ubiquitous AI—An overview on history, evolution, and upcoming challenges in AI implementation. *Micromachines, 12(6), 665*.
88. Khan, O. U., Abdullah, S. M., Olajide, A. O., Sani, A. I., Faisal, S. M. W., Ogunola, A. A., & Lee, M. D. (2024). The Future of Cybersecurity: Leveraging Artificial Intelligence to Combat Evolving Threats and Enhance Digital Defense Strategies. *Journal of Computational Analysis and Applications, 33(8)*.
89. Kinyua, J., & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing, 28(2)*.
90. Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. *Communications on Applied Electronics*, *7*(7), 8-13.
91. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7, 8176-8186*.
92. Lehmann, H. (2023). AI-Based ChatOps: Enhancing Collaboration and Incident Response in DevOps Teams.
93. Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *Cyber Resilience of Systems and Networks*, 1-25.
94. Loaiza, F. L., Birdwell, J. D., Kennedy, G. L., & Visser, D. (2022). Utility of artificial intelligence and machine learning in cybersecurity. *Institute for Defense Analyses*.
95. Lu, H., Chen, W., Zhou, C., Wu, H., Lyu, F., & Shen, X. S. (2024). A Two-Dimensional Hybrid Federated Learning Framework for Secure Data Cooperation of Multiple Network Service Providers. *IEEE Wireless Communications*.
96. Maezo, R. G., & Rey, A. E. (2023, June). Boosted CSIRT with AI powered open source framework. In *2023 JNIC Cybersecurity Conference (JNIC)* (pp. 1-8). *IEEE*.
97. Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics, 1-28*.
98. Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News, 190(1), 1-69*.
99. Manoharan, A., & 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.
100. Mardikoraem, M. (2024). Navigating Protein Fitness Landscapes With Machine Learning and Biological Insights (Doctoral dissertation, Michigan State University).
101. Markowitz, D. M., Boyd, R. L., & Blackburn, K. (2024). From silicon to solutions: AI's impending impact on research and discovery. *Frontiers in Social Psychology, 2*, 1392128.
102. McCoy, C. G. (2022). A relevance model for threat-centric ranking of cybersecurity vulnerabilities (Doctoral dissertation, Old Dominion University).
103. Mohammadi, R., Hosseini, M. M., & Bahrami, R. (2025a). Uncovering security vulnerabilities through multiplatform malware analysis. *Security and Privacy, 8(1), e455*.
104. Mohammadi, R., Hosseini, M. M., & Bahrami, R. (2025b). *(If this truly is a second, distinct reference—use (2025a) vs. (2025b) to differentiate in APA style. Adjust as needed.)*
105. Mokhtarian, I. (2024). Utilizing Process Mining and Deep Learning to Detect IoT/IIoT Cyberattacks–A Hybrid Approach (Doctoral dissertation, University of Illinois at Chicago).
106. Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions. *IEEE Communications Surveys & Tutorials, 25(3), 1775-1807*.
107. Noshi, A., & Blaser, F. (2024). Integrating Artificial Intelligence and Machine Learning for Advanced Cyber Security in SOC Operations.
108. Nespoli, P., Papamartzivanos, D., Mármol, F. G., & Kambourakis, G. (2017). Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. *IEEE Communications Surveys & Tutorials, 20(2), 1361-1396*.
109. Ohagen, P., Lins, S., Thiebes, S., & Sunyaev, A. (2022). Using ChatOps to achieve continuous certification of cloud services.
110. Oluwawemimo, E. (2024). The Role of Artificial Intelligence in Incident Response for Digital Domain SMEs.
111. Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. *Comput. Eng. Intell. Syst*, *4*, 50-57.
112. Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service. *International Journal on Computer Science and Engineering (IJCSE)*, 760-769.
113. Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEE Access, 12, 12229-12256*.
114. Paesano, A. (2023). Artificial intelligence and creative activities inside organizational behavior. *International Journal of Organizational Analysis, 31(5), 1694-1723*.
115. Perkola, P. (2024). Preparing for NIS2 directive reporting obligations with ISO 27001.
116. Prabhavalkar, R., Hori, T., Sainath, T. N., Schlüter, R., & Watanabe, S. (2023). End-to-end speech recognition: A survey. *IEEE/ACM Transactions on Audio, Speech, and Language Processing, 32, 325-351*.
117. Prasad, S., & Kulkarni, P. (2023, September). Role of artificial intelligence in business process transformation. In *AIP Conference Proceedings (Vol. 2736, No. 1). AIP Publishing*.
118. Radanliev, P., De Roure, D., Van Kleek, M., Santos, O., & Ani, U. (2021). Artificial intelligence in cyber physical systems. *AI & Society, 36(3), 783-796*.

119. Rao, S. M., & Jain, A. (2024). Advances in Malware Analysis and Detection in Cloud Computing Environments: A Review. *International Journal of Safety & Security Engineering, 14(1)*.
120. Rath, S., Das, N. R., & Pattanayak, B. K. (2024). Stacked BI-LSTM and E-optimized CNN-A hybrid deep learning model for stock price prediction. *Optical Memory and Neural Networks, 33(2), 102-120*.
121. Redhu, A., Choudhary, P., Srinivasan, K., & Das, T. K. (2024). Deep learning-powered malware detection in cyberspace: a contemporary review. *Frontiers in Physics, 12, 1349463*.
122. Rezaei, M., Pironti, M., & Quaglia, R. (2024). AI in knowledge sharing, which ethical challenges are raised in decision-making processes for organisations? *Management Decision*.
123. Safitra, M. F., Lubis, M., & Kurniawan, M. T. (2023, March). Cyber resilience: research opportunities. In *Proceedings of the 2023 6th international conference on electronics, communications and control engineering* (pp. 99-104).
124. Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11(1), 105*.
125. Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing, 76, 5320-5363*.
126. Samson, B. P. V., & Sumi, Y. (2019, May). Exploring factors that influence connected drivers to (not) use or follow recommended optimal routes. In *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1-14).
127. Sangaroonsilp, P. (2024). Supporting the Development and Management of Privacy-Aware Software Applications (Doctoral dissertation, University of Wollongong).
128. Santos, O., Salam, S., & Dahir, H. (2024). The AI revolution in networking, cybersecurity, and emerging technologies.
129. Sarker, I. H. (2024). AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. *Springer Nature*.
130. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science, 2(3), 173*.
131. Sarker, I. H., Hoque, M. M., Uddin, M. K., & Alsanoosy, T. (2021). Mobile data science and intelligent apps: concepts, AI-based modeling and research directions. *Mobile Networks and Applications, 26(1), 285-303*.
132. Sharma, A., & Spunda, R. (2025). SOC Optimization Through AI-Powered Automation and Blockchain Integration.
133. Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. K. (2022). Orchestration of APT malware evasive manoeuvers employed for eluding anti-virus and sandbox defense. *Computers & Security, 115, 102627*.
134. Shin, Y. C., & Xu, C. (2017). Intelligent systems: modeling, optimization, and control. *CRC Press*.
135. Singh, B. (2024). Unmanned Aircraft Systems (UAS), Surveillance, Risk Management to Cybersecurity and Legal Regulation Landscape: Unraveling the Future Analysis, Challenges, Demand, and Benefits in the High Sky Exploring the Strange New World. *Unmanned Aircraft Systems*, 313-354.
136. Singh, B., & Kaunert, C. (2025). Intelligent Machine Learning Solutions for Cybersecurity: Legal and Ethical Considerations in a Global Context. In *Advancements in Intelligent Process Automation* (pp. 359-386). *IGI Global*.
137. Singh, J., & Singh, J. (2021). A survey on machine learning-based malware detection in executable files. *Journal of Systems Architecture, 112, 101861*.
138. Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews, 21(2), 1720-1736*.
139. Spinner, A. D. (2024). Deep Generative Models for Prediction and Design of Enzymes (Doctoral dissertation, Harvard University).
140. Staves, A. J. (2023). Operational Technology Preparedness: A Risk-Based Safety Approach to Scoping Security Tests for Cyber Incident Response and Recovery. *Lancaster University (United Kingdom)*.
141. Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A cyber incident response and recovery framework to support operators of industrial control systems. *International Journal of Critical Infrastructure Protection, 37, 100505*.
142. Surampudi, Y. (2024). Big Data Meets LLMs: A New Era of Incident Monitoring. *Libertatem Media Private Limited*.
143. Tan, K., Wang, Z. Q., & Wang, D. (2022). Neural spectrospatial filtering. *IEEE/ACM Transactions on Audio, Speech, and Language Processing, 30, 605-621*.
144. Thomas, C., & Kovashka, A. (2019). Artistic object recognition by unsupervised style adaptation. In *Computer Vision–ACCV 2018: 14th Asian Conference on Computer Vision, Perth, Australia, December 2–6, 2018, Revised Selected Papers, Part III 14* (pp. 460-476). *Springer International Publishing*.
145. Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security, 23(3), 1695-1719*.
146. Vijayalakshmi, P. S., & Jayakumar, M. (2024). Deep Neural Networks for Automated Cyber Security: Identification of Dynamic Malware in Cloud Computer Networks. In *Leveraging Artificial Intelligence (AI) Competencies for Next-Generation Cybersecurity Solutions* (pp. 139-173). *Apple Academic Press*.
147. Vu, T. H., Jagatheesaperumal, S. K., Nguyen, M. D., Van Huynh, N., Kim, S., & Pham, Q. V. (2024). Applications of generative AI (GAI) for mobile and wireless networking: A survey. *IEEE Internet of Things Journal*.
148. Waqas, M., Tu, S., Halim, Z., Rehman, S. U., Abbas, G., & Abbas, Z. H. (2022). The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. *Artificial Intelligence Review, 55(7), 5215-5261*.
149. World Health Organization. (2023). *Pedestrian safety: a road safety manual for decision-makers and practitioners. World Health Organization*.
150. Wu, C., Wei, X., Li, S., & Zhan, A. (2023). Mstpose: learning-enriched visual information with multi-scale transformers for human pose estimation. *Electronics, 12(15), 3244*.
151. Yazici, İ., Shayea, I., & Din, J. (2023). A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems. *Engineering Science and Technology, an International Journal, 44, 101455*.
152. Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A. (2013a). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. *Journal of Engineering, Computers & Applied Sciences (JEC&AS), 2*(7).
153. Yeboah, D. T., Odabi, I., & Abilimi Odabi, M. C. A. A. (2016). *Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment*.
154. Yeboah, T., Opoku-Mensah, E., & Abilimi, C. A. (2013b). Automatic Biometric Student Attendance System: A Case Study Christian Service University College. *Journal of Engineering Computers & Applied Sciences*, 2(6), 117-121.
155. Yeboah T. & Abilimi C.A. (2013). *Using Adobe Captivate to creative Adaptive Learning Environment to address individual learning styles: A Case study Christian Service University*, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181,www.ijert.org, "2(11).
156. Younis, H., Sundarakani, B., & Alsharairi, M. (2022). Applications of artificial intelligence and machine learning within supply chains: systematic review and future research directions. *Journal of Modelling in Management, 17(3), 916-940*.
157. Yousaf, Z., & Boomsma, D. (2024). AI-Driven SOC Operations: Improving Incident Response Time and Threat Analysis.
158. Yu, C., Zezario, R. E., Wang, S. S., Sherman, J., Hsieh, Y. Y., Lu, X., ... & Tsao, Y. (2020). Speech enhancement based on denoising autoencoder with multi-branched encoders. *IEEE/ACM Transactions on Audio, Speech, and Language Processing, 28, 2756-2769*.
159. Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *IEEE Access, 9, 94668-94690*.
160. Zhang, G., Zhong, B., Liang, Q., Mo, Z., Li, N., & Song, S. (2024). One-stream stepwise decreasing for vision-language tracking. *IEEE Transactions on Circuits and Systems for Video Technology*.

161. Zhang, J., Xie, Y., Ding, W., & Wang, Z. (2023). Cross on cross attention: Deep fusion transformer for image captioning. *IEEE Transactions on Circuits and Systems for Video Technology, 33(8), 4257-4268*.

162. Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access, 10, 93104-93139*.