World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Harnessing the power of artificial intelligence to enhance next-generation cybersecurity

Sheetal Temara *

Department of Computer and Information Sciences, University of the Cumberlands, 6178 College Station Drive, Williamsburg, KY 40769.

World Journal of Advanced Research and Reviews, 2024, 23(02), 797–811

Publication history: Received on 02 July 2024, revised on 07 August 2024, and accepted on 10 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2428

Abstract

Cybersecurity ecosystem is an important facet in protecting sensitive information and securing critical infrastructure for countering modern cyber threats. With the increasing complexity and frequency of security incidents, there is an escalating demand for development of innovative solutions beyond current human capabilities pertaining to cybersecurity measures. Artificial Intelligence or AI can be utilized in a myriad of areas of cybersecurity. It emerged as a technological innovation to enhance cyber protection by facilitating faster and real-time threat detection for known and unknown threats, automating processes to minimize human error, and optimal decision-making. Harnessing the power of AI in cybersecurity creates formidable defense capabilities against the constantly changing cyber threats of future while empowering the cybersecurity personnel with threat intelligence and proactive foresight to safeguard critical assets and confidential information with unparalleled precision and effectiveness. This research paper aims to investigate the potential of AI-enabled cybersecurity systems and focuses on deducing the benefits of using AI in enhancing cybersecurity processes for organizations seeking to manage their risk profile. Through a comprehensive literature review, the wide-ranging applications of AI in cybersecurity have been analyzed such as intrusion detection, predictive simulation, and automated emergency response management. The study examines the benefits of implementing AI-based cyber defenses such as improved promptness and accuracy in vulnerability assessment and threat management, reduced false positives, and recognize patterns. The future potential of AI in cybersecurity will take a leap forward in expanding protection mechanisms to evaluate the strengths and weaknesses of attack vectors to prevent an adversarial attack.

Keywords: Cybersecurity; Artificial intelligence; Threat; Probability

1. Introduction

Artificial intelligence (AI) can be described as a system that recognizes its surroundings and performs activities increasing the probability of successful completion of objective. AI is an amalgamation of physical intelligence and technology which can be used to obtain desired results. This concept supplies apparatus for resolving complicated and arduous challenges on a computer system [1]. Improved information security controls with embedded AI are beginning to be used to protect organizations from progressively capable threat actors. The motive of AI is to facilitate the ability for computer systems to impersonate the cognitive thinking capabilities of humans in order to replicate their behavior to resolve challenges more expeditiously and effectively than can be accomplished by individuals. Numerous activities including strategizing, migrating, communicating, target and noise identification, creative pursuits, and company operations can be performed by AI [4]. Many methods that can be performed by AI are also relevant to resolving issues in the field of cybersecurity including natural language processing (NLP), machine learning, computational linguistics, and analytics that are both extrapolative and instructive in nature. Typically, AI solutions build their knowledge base through data provided by professionals or generated from transactions executed in existing systems. As additional data

* Corresponding author: Sheetal Temara

is provided to the AI systems which results in gradually more accurate replies which will ultimately surpass human subject matter experts. Within cybersecurity, AI is built from machine learning techniques in order to both recognize and mitigate risks by classifying inbound information as reliable or nefarious [6]. AI can be trained in a few different ways including supervised learning which is when the administrator controls the learning activities of the system, unsupervised learning which is when patterns are identified by the system, and reinforcement learning which makes use of trial and error to resolve issues without feeding the system data.

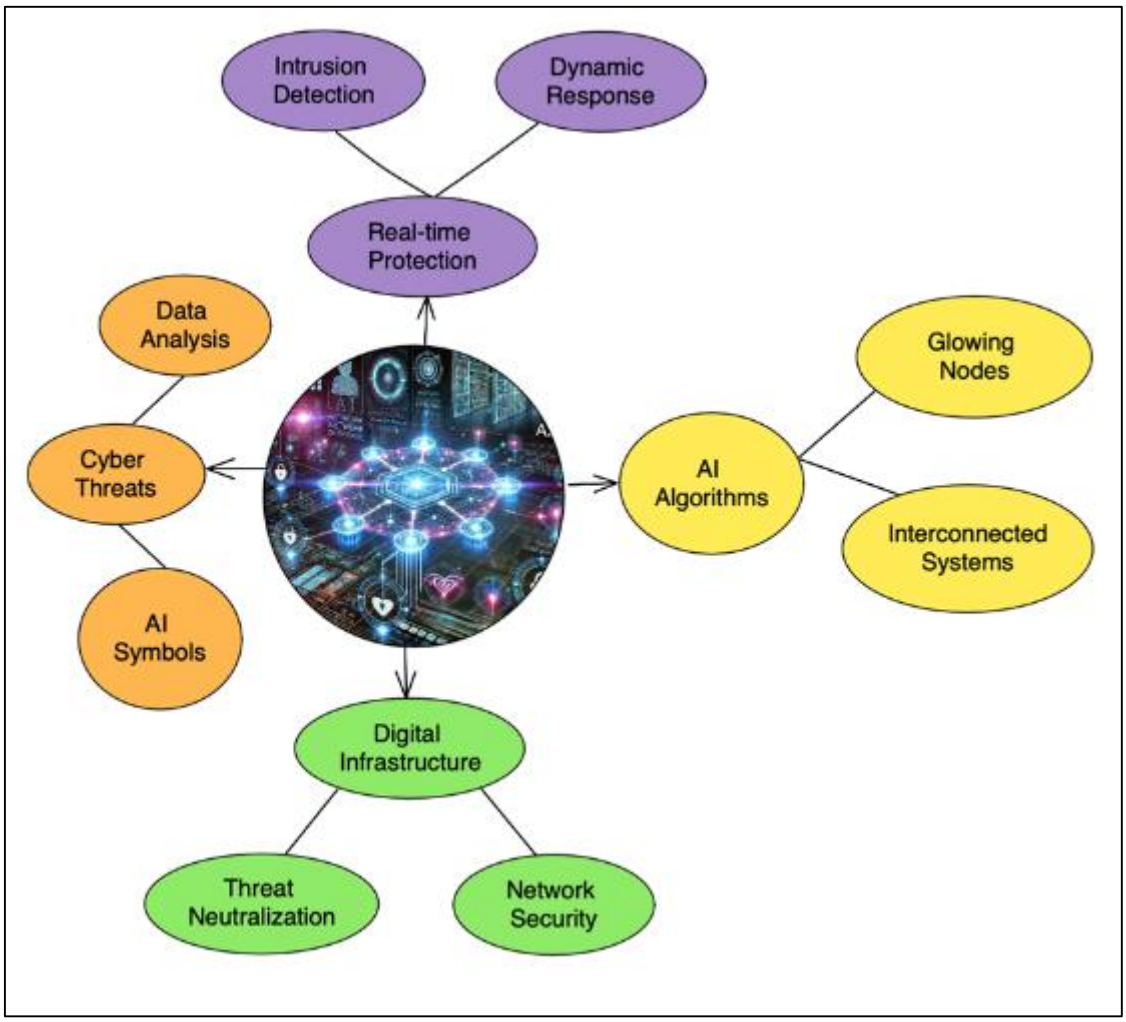

Figure 1 Futuristic Cybersecurity Defense System

1.1. The Role of Artificial Intelligence in Cybersecurity

Cybersecurity encompasses a wide variety of subjects in information security from personal computers to disaster recovery to security awareness training which carries a robust connection with AI. Cybersecurity personnel face several challenges in the current era including insufficient quantity of resources, increased sophistication of threat actors including nation-states, deficiencies of expertise, unrestrained movement of transactional information, and insufficient time to perform their assigned work [7]. Cybersecurity incidents are growing at a significant rate including the negative effects which has increased the need for enhanced security controls. There are several areas of cybersecurity that AI can provide assistance in order to meet the challenges above including the formulation of preprogrammed replies, expediting analysis of behavioral anomalies, and increasing accuracy of threat detection, organizing threat response operations [15]. The cybersecurity controls at an organization can be improved tremendously with the integration of AI including spam prevention, vulnerability discovery, and the categorization of information as malicious or benign [9]. Some of the cybersecurity activities that can be enhanced using AI include intrusion prevention, Security Operations Centre (SOC) monitoring, rapid vulnerability remediation, and Dark Web surveillance in order to obtain threat intelligence.

1.2. Areas of Cybersecurity that can be Improved with AI

Cybersecurity is expected to evolve due to AI given the capability it exhibits to identify inconsistencies and identify risks which can be used to protect against novel and inconspicuous attacks with increased efficiency and responsiveness required to manage threats that are developing. Some of the facets of cybersecurity that can be enhanced with machine learning and additional AI strategies include intrusion detection, strategic cyber readiness, as well as vulnerability identification, heuristic analysis, exploit development, and detection of malware mutation.

1.3. Benefits of AI in Cybersecurity

There are several benefits that AI provides to cybersecurity. Incident response can be transformed with AI to be more efficient with a higher velocity response time. False positives can create additional overhead for security operations teams as each potential threat has to be researched [8]. AI can decrease the load on the SOC teams by lowering the number of false positives produced by contemporary threat detection systems. In a similar vein, AI induced machine learning facilitates results with greater validity than contemporary threat detection systems. AI can supply extensive overview of an incident. AI also has lower reliability on direct human configuration as it can create its own security signatures that are more successful preventing novel security threats. Security systems that are enabled with AI can provide analysts with time to work on other endeavors that AI cannot perform. Detection of unknown attacks is a key competence of AI. AI has the ability to evolve to novel risks by learning from previous events which means that security controls can develop to become more intelligent and successful overtime lowering the probability of security issues moving forward [10]. Many recurring and laborious cybersecurity situations can be automated with AI comprising of incident handling and threat detection. Cybersecurity operations can be transformed in order to keep up with the increasing demand for security defenses. AI algorithms preemptively discover security issues and risks prior to exploitation assisting organizations to prevent security events prior to their manifestation [12]. AI can also aid with real-time customization of web filtering to provide a security control for individuals in order to protect them from malicious content and web properties. AI can be integrated with the DevOps pipeline to build more intelligent and secure code.

1.4. Evolution of Cybersecurity with AI

Greater flexibility is offered by AI systems to adjust to evolving scenarios in a constantly changing threat landscape. Some functions are available from AI to counteract cyberattacks. One function is anomaly prediction which sifts through the data in order to prognosticate the identification of security issues and assist with shoring up defensive controls to protect against specific attacks [17]. Another tool that AI provides is called anomaly detection which can identify abnormalities with applications, web properties, and network infrastructure with the further ability to trigger alerts for additional investigation and preventative measures. The last AI tool against cyberattacks is referred to as attack response which will block attacks instantaneously without human interference [19].

2. Literature Review

This paper analyzed the benefits of cybersecurity AI described in the following literature: Reinventing Cybersecurity with Artificial Intelligence by Tolido et al. [2], AI and automation for cybersecurity: How leaders succeed by uniting technology and talent by Muppidi et al. [3], Consideration of Artificial Intelligence for Cybersecurity Aspects of I&C Systems by Zid et al. [6], Cyber and AI: 2021 Technology Spotlight by Booz Allen Hamilton et al. [11], Implications of Artificial Intelligence for Cybersecurity by Johnson & Grumbling [12], Currently Deployed Artificial Intelligence and Machine Learning Tools for Cyber Defense Operations by Krasser et al. [13], Balancing Power and Protection: AI in Cybersecurity and Cybersecurity in AI by PricewaterhouseCoopers [14], Providing Cyber Security using Artificial Intelligence – A survey by Sagar et al. [15], Artificial intelligence in the cyber security environment Artificial intelligence in the cyber security environment by Vähäkainu et al. [16].

2.1. Reinventing Cybersecurity with Artificial Intelligence by Tolido et al. [2]

As the attack surface expands due to a continuously changing technology landscape, an argument is made that security problems are becoming more complicated [2]. Several AI use cases for cybersecurity are discussed including those for detection, prediction, and cyber threat response. Prioritization is needed to determine the most valuable security strategy use cases and integration points for organizations deploying AI in order to make the best use out of the potential of AI as studied by Tolido et al. [2]. After the AI use cases are ranked, it is noted that a roadmap should be constructed to create a timeline for implementation of the AI security strategy use cases [2].

2.2. AI and automation for cybersecurity: How leaders succeed by uniting technology and talent by Muppidi et al. [3]

The volume of security incidents and attack surfacer are continuing to increase mandating a new method for managing the increase as presented by Muppidi et al. [3]. AI has been identified as a security tool that can provide an effective yet cost efficient approach to handle the growth in security attacks [3]. Muppidi et al. [3] examines that several cybersecurity related use cases for AI integration are noted to be high priority use cases for protection and prevention to enhance security operation performance including endpoint discovery and asset management, vulnerability and patch management, access management, threat simulation, identity management, automated detection and response, threat intelligence, case management, threat management, and behavior modeling and anomaly detection. An argument is also made by Muppidi et al. [3] that a roadmap should be created to design a roadmap for AI implementations to flush out the overall security strategy.

2.3. Consideration of Artificial Intelligence for Cybersecurity Aspects of I&C Systems by Zid et al. [5]

A reason is stated by Zid et al. [5] that security related AI applications can provide many advantages, but that AI integrations can lead to additional problems. AI implementations can be used to manage and mitigate normal attack methods that traditional cybersecurity controls have reduced success in stopping [5]. Three main goals are mentioned by Zid et al. [5] that AI algorithms can be applied to including creating predictions, planning preventions, and taking actions. Preconditions are outlined for the use of AI in order to establish a successful implementation [5].

2.4. Cyber and AI: 2021 Technology Spotlight by Booz Allen Hamilton et al. [11]

AI with Machine Learning is expected to augment security controls by empowering human related security processes with AI generated information as evaluated by Booz Allen Hamilton et al. [11]. Three core processes are discussed as areas that should be considered for AI augmentation including attack detection with early discovery and identification of learned patterns for malicious activity, behavior analysis to rapidly identify dubious actions including zero-day type attacks, and risk assessment of identified threats [11]. Several benefits of integration AI with cybersecurity are identified by Booz Allen Hamilton [11] including free security personnel to work on higher priority tasks with AI automation, real cost savings through swifter response and prevention of incidents caused by attacks, and time saving by quickly rating risks for prioritization of security personnel follow-up activities.

2.5. Implications of Artificial Intelligence for Cybersecurity by Johnson & Grumbling [12]; Currently Deployed Artificial Intelligence and Machine Learning Tools for Cyber Defense Operations by Krasser et al. [13]

A novel approach was explained by Johnson & Grumbling; Krasser et al. [12, 13] for identifying anomalies regarding unauthorized access to files to offset the difficulty commonly encountered with maintaining access control lists (ACLs). The study argues that inadvertent access to documents can commonly occur in use cases involving employees changing roles within an organization [12, 13]. The new design by Johnson & Grumbling; Krasser et al. [12, 13] discussed incorporates AI and is considered more dynamic as it monitors for unauthorized access requests using machine learning data enrichment. This model considers two inputs during learning including user specific data and document specific data in order to determine if a specific request for access is anticipated behavior or abnormal behavior [12, 13]. In addition, an automated approach to manage “zero-day phishing” as well as a second approach to empower humans with AI produced information to make decisions related to the identification and blocking of phishing emails as provided by Johnson & Grumbling; Krasser et al. [12, 13]. Both of these are expected to eliminate phishing as a successful attack type in the next few years [12, 13].

2.6. Balancing Power and Protection: AI in Cybersecurity and Cybersecurity in AI by PricewaterhouseCoopers [14]

The evolution of technology as studied by PricewaterhouseCoopers [14] has expanded the threat landscape and induced an intensification of attacks making AI an essential cybersecurity control element. AI is produces advanced cybersecurity controls enhancing four primary subjects including incident management, self-decisioning which can compile and create automated responses, accelerated investigations, and accurate threat detection capabilities [14]. An argument is made by PricewaterhouseCoopers [14] that enhancements provided by AI empower security systems to sense in order to discover anomalous behaviors, think by using constantly training to learn and later discover true malicious behavior to decrease false positives and increase identification of true attacks, and act to mitigate vulnerabilities and provide alerting. Lastly, an argument is made that AI is evolving to use machine learning in order to enhance threat detection, that phishing discovery and avoidance will further be enhanced with AI, that vulnerability management will become simpler with AI integration, and that authentication capabilities will be improved with more formidable password protection powered by AI [14].

2.7. Providing Cyber Security using Artificial Intelligence – A survey by Sagar et al. [15]

According to Sagar et al. [15], AI enables early alerting prior to hackers compromising information while some AI solutions actively secures data. Humans are required to constantly provide AI implementations tuning and training [15]. Several different types of AI solutions for Cybersecurity are examined by Sagar et al. [15] including threat mitigation, security decision-making, defense enhancement, security optimization, and data mining for analytics.

2.8. Artificial intelligence in the cyber security environment Artificial intelligence in the cyber security environment by Vähäkainu et al. [16]

Vähäkainu et al. [16] stated that data regarding a variety of artificial intelligence implementations covering several fundamental cyber security topics including operational security, security incident response, cyber threat intelligence, web application security, infrastructure security, mobile application security, and endpoint security was reviewed to understand threat coverage for each. As human investigation of cyber security events is intensive and laborious, the study argues that novel solutions that are efficient are needed to enable organizations to manage the massive number of alerts that are generated [16]. Anomalies can be discovered immediately and at an earlier stage using artificial intelligence based solutions. On the other hand, contemporary information security controls have trouble managing many of today's attack patterns as provided by Vähäkainu et al. [16]. Artificial intelligence is claimed to provide the capability to manage a variety of attacks while producing concise well-prepared reporting as a basis for making decisions while facilitating collaboration with AI solutions and cyber security analysts [16].

3. Research Methodology

The content of this section examines the resources used to acquire the data analyzed in this study, the factors used to determine the documents included in this study, the approach for evaluating and establishing the results. The research questions provided below contains the primary goals of this paper.

- RQ1: What are the current challenges in cybersecurity that could benefit from augmentation?
- RQ2: What properties of artificial intelligence can benefit cybersecurity?
- RQ3: How can these artificial intelligence properties be integrated with cybersecurity in such a way as to improve the current posture of the security controls?
- RQ4: What are some specific artificial intelligence driven solutions that have been identified to benefit cybersecurity controls?

Quality reference articles were required for this systematic literature review identified with the research questions in order to reduce the criteria for article selection. The research process relied heavily on the evolving academic literature and publicly available author blog posts and news articles on AI in cybersecurity. A total of 33 different articles including scholarly journals, conference papers, technical reports, special edition tutelages, theoretical forum posts were gathered in April 2023 for the purpose of conducting research on how AI can enhance the field of cybersecurity. All articles emphasized on AI in cybersecurity and its implications and were published in the years ranging from 2019-2023. Making use of the subject areas from the questions above, Google Scholar, IEEE Xplore, ResearchGate and UC's Grover M. Hermann Library were utilized to find reliable scholarly resources. Also, the same subject from the questions were used in search requests to identify author blog posts and independent news articles. During the investigation of the articles located using these searches, an evaluation was performed on each resource using the relevance to the research subjects pertinent to artificial intelligence and cybersecurity.

4. Results and Discussion

The following section unravels the significant role that AI can facilitate in cybersecurity by exploring the technical and procedural perspective employed in researching the study. The subsequent analysis comprises of a detailed examination of the key elements contributing to leveraging artificial intelligence in the realm of cybersecurity which laid the substance for additional exploration on the positive impact of AI.

4.1. Endpoint Security

Endpoint protection systems is the most frequent type of machine learning (ML) deployed today. AI can be successful in access control for endpoints by utilizing machine learning to understand prior behavioral blueprints in order to

generate risk scores. AI can also be effective at controlling security of mobile endpoints through the use of machine learning and zero-trust methodology. Asset management can be a critical issue for organizations as misclassified assets could result in these assets not being included in the scope of critical security controls [18]. AI can enhance information technology (IT) asset management by taking advantage of key capabilities of machine learning. Machine learning can be positioned to decide the safety level of applications and isolating them from other applications in production environment as the levels of safety drop. Organizations can be empowered to forecast, identify, and react to illicit behaviors resulting from the integration of AI and machine learning. Local-to-end points, execution of instantaneous scans of every process with unfamiliar reputation can be performed by AI solutions and powered with machine learning to enhance security [20]. Machine learning can ensure that endpoints are compliant with regulatory requirements and organizational policies by observing behaviors regarding data access and data transmission.

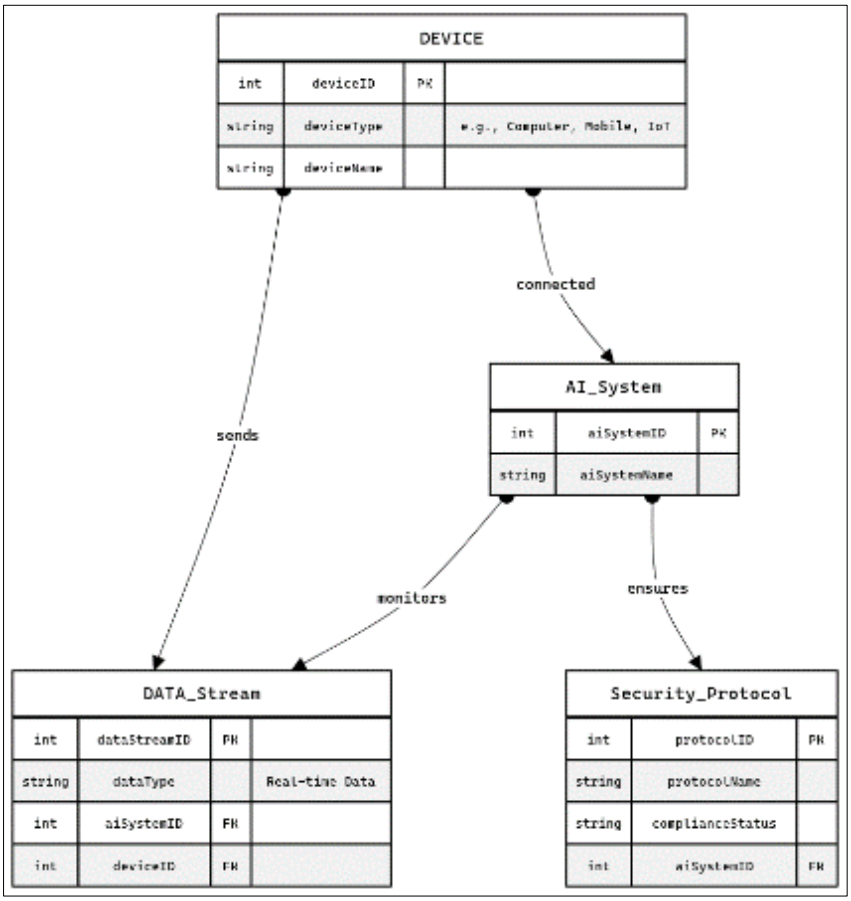

Figure 2 AI-powered endpoint security system

This entity-relationship diagram represents an AI-powered endpoint security system where multiple devices such as computers, mobile phones, and IoT devices are connected to a central AI system that monitors and safeguards them.

Each device is uniquely identified by a deviceID and is categorized by its deviceType (e.g., computer, mobile, IoT) with a specific deviceName. These devices are connected to the AI system represented by the AI_System entity which has its own unique identifier aiSystemID, and a name aiSystemName. The AI system continuously monitors real-time data streams sent by the connected devices. These data streams are represented by the DATA_Stream entity which includes the dataStreamID to uniquely identify each stream, the type of data being analyzed (dataType), and foreign keys (aiSystemID and deviceID) linking the data stream back to both the AI system and the originating device.

The AI system also ensures that each device complies with specific security protocols represented by the Security_Protocol entity. This entity includes a protocolID for unique identification, a protocolName, and a complianceStatus indicating whether the device adheres to the protocol. The AI system plays a critical role in ensuring compliance by enforcing these protocols across all connected devices. The relationships in the diagram highlight how devices send data to the AI system which then monitors these data streams and ensures security compliance thus preventing unauthorized access and maintaining the integrity of the network.

4.2. Threat Classification

As the challenges in cybersecurity grows, organizations are discovering that AI can add tremendous value in daily security operation regime. There are multiple areas of cybersecurity that AI can enhance which are currently managed using extreme human capital. Novel cyber threats can be discovered by AI through the behavioral analysis of data generating within an organization by networks, computing resources, applications, data sources, and security controls in order to facilitate the rapid response to the threats. As the attack surface has continued to increase including the cloud, mobile devices, IoT devices as well as the classical network and computing endpoints, organizations are obligated to build a larger array of security controls with the addition of new monitoring requirements. The amount of data generated from the broader attack surface and extended security controls in order to enable the monitoring has also significantly grown requiring an extreme time commitment from security personnel in order to identify behaviors of threat actors and patterns related to attack traffic [21]. As the available security personnel and time are limited resources to monitor the various security controls, AI can provide an amplification to resource limitations in order to automate the identification of threats by performing data filtering, eliminating false positives as well as enhancing the data itself which will greatly alleviate the difficulty in analyzing large amounts of data required for current strategies of security operations. AI solutions provides enhanced automation with added efficiency that frees up security personnel to work on other mission-critical responsibilities [24]. Discovery of a new blueprint for malicious activity can be correlated with preexisting bad blueprints to determine the likelihood that the data is of illicit intent with greater efficiency and precision than security personnel can perform. Analysis can also be performed by AI in order to associate data from the various origin points to create an illustration of ongoing malicious actions to enable security personnel to fully comprehend the full extent of the attack.

4.3. Risk Analysis

After a threat has been identified, a risk assessment must be performed in order to understand the actual risk of the threat with the lens focusing on any existing security controls overlapped on top of the identified threat. Understanding this risk allows security teams to understand the potential effect this threat could have on the organization's operations and allows the response team to determine the appropriate course of action required for remediation [23]. AI with machine learning can assist with the risk assessment process in order to guide a proper reaction to the threat identified with the appropriate context understanding the current organizational security ecosystem.

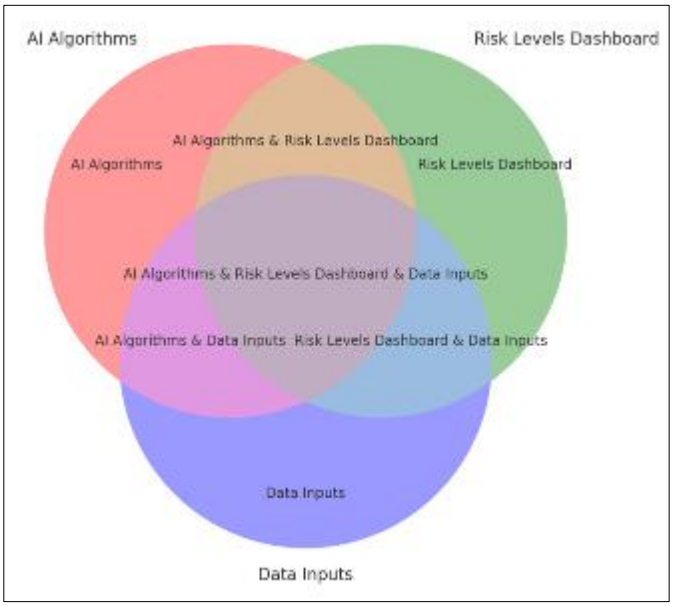

Figure 3 AI Risk Analysis within an organization's IT environment

The venn diagram shows the intersection between AI algorithms, risk levels dashboard, and data inputs depicting how these elements interact. It visually represents a dashboard with AI algorithms assessing and categorizing threats based on data inputs from various sources.

4.4. Remediation Guidance

Using machine learning, AI solutions can create security rubrics and signatures making them self-sufficient and less contingent on human configuration while becoming more successful in blocking novel threats. Security personnel allocate much of their working time toward applying patches which is becoming an extremely tedious process in terms of both time and resource management [22]. AI can lower risk through a patch management implementation that automates the discovery, prioritization, and remediation of vulnerabilities excluding excessive manual work. In the current environment, after the risk is understood regarding the threat, real-time security event alerts can be triggered with automated procedures in order to kick off remediation activities by humans to address identified security issues in a prudent timeframe. Machine Learning can also be utilized in order to appropriately analyze security control related data in order to identify threats, subsequently machine learning can be recruited to perform substantial processing driven by monitoring and evaluating previous actions performed by human security analysts. This training of the AI engine can augment the system's capability to orchestrate remediation activities. Recurring actions can also be automated by AI and machine learning. This use case would cover notifications when remediation actions need to be expedited with a low-risk of error and where the AI platform has high confidence regarding the threat [25]. This capability provides much needed relief given the industry deficiency of experienced cybersecurity experts.

4.5. Automated Malware Detection

Software whose goal is to interfere with a company's infrastructure through exploitation of attached devices [28]. Using machine learning, AI systems can automatically detect brand new malware through analysis of empirical data where traditional malware identification makes use of signature matching. Patterns in previous security incidents and related alerts can be discovered using AI which will enhance the currently deployed security strategy as well as defend an organization's infrastructure from this attack in future.

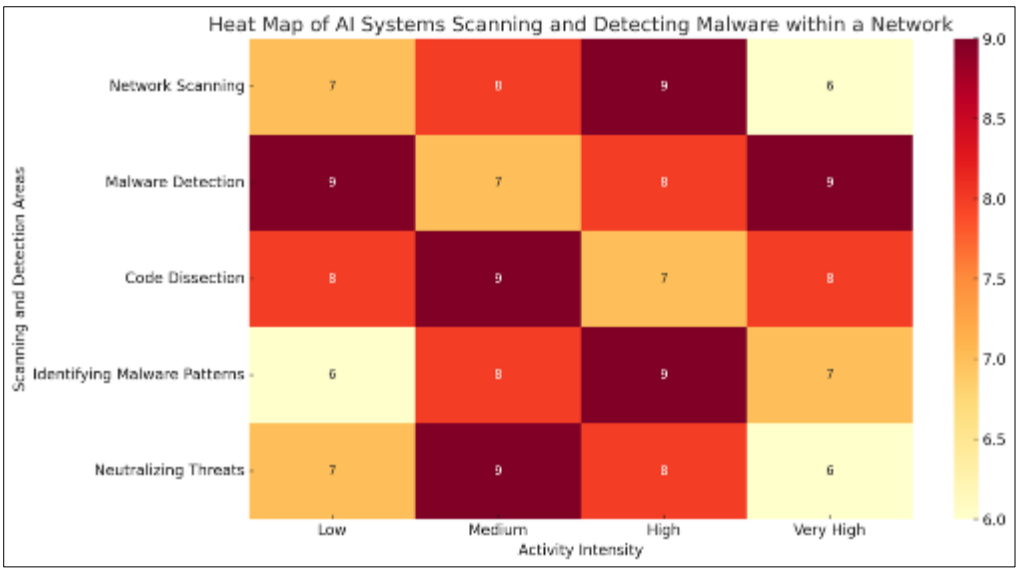

Figure 4 AI Systems Scanning and Detecting Malware

This heat map diagram represents the intensity of AI systems' activities in scanning and detecting malware within a network. The heat map is divided into rows with each representing a specific activity related to malware detection and columns that indicate the level of intensity for those activities.

4.5.1. Rows (Activities)

- Network Scanning represents the efforts of AI to scan the network for any signs of malicious activity or vulnerabilities.
- Malware Detection focuses on the detection of malicious code within the scanned data.
- Code Dissection shows the role of AI in analyzing and breaking down detected code to understand its structure and behavior.

- Identifying Malware Patterns: Reflects AI's use of machine learning to recognize patterns that indicate new or evolving types of malware.
- Neutralizing Threats involves AI taking actions to neutralize detected threats and prevent them from causing harm.

4.5.2. Columns (Activity Intensity)

- Low represents minimal activity in the corresponding area.
- Medium indicates a moderate level of activity.
- High shows a high level of AI activity in the specified area.
- Very High denotes intense AI activity likely focused on critical tasks such as real-time threat neutralization.

4.5.3. Heat Map Colors

- Lighter Colors (Yellow/Orange): These indicate lower intensity levels of AI activity in those specific areas.
- Darker Colors (Red): Represent higher intensity levels, where AI is more actively engaged in scanning, detecting, or neutralizing threats.

4.6. Social Engineering Discovery

Social engineering related incidents which take advantage of the weakness of humans tendency to believe that the interactions are authentic and lack of cyber awareness. AI systems can utilize deep learning models to simulate human analysis can evaluate unstructured data that has not been classified in order to learn independently. This AI model is more successful in discovering and mitigating attacks involving social engineering than conventional systems such as Secure Email Gateway (SEG). One other function that can be provided by AI is a phishing simulation to quiz users with simulated social engineering attacks for educational training, and awareness purposes.

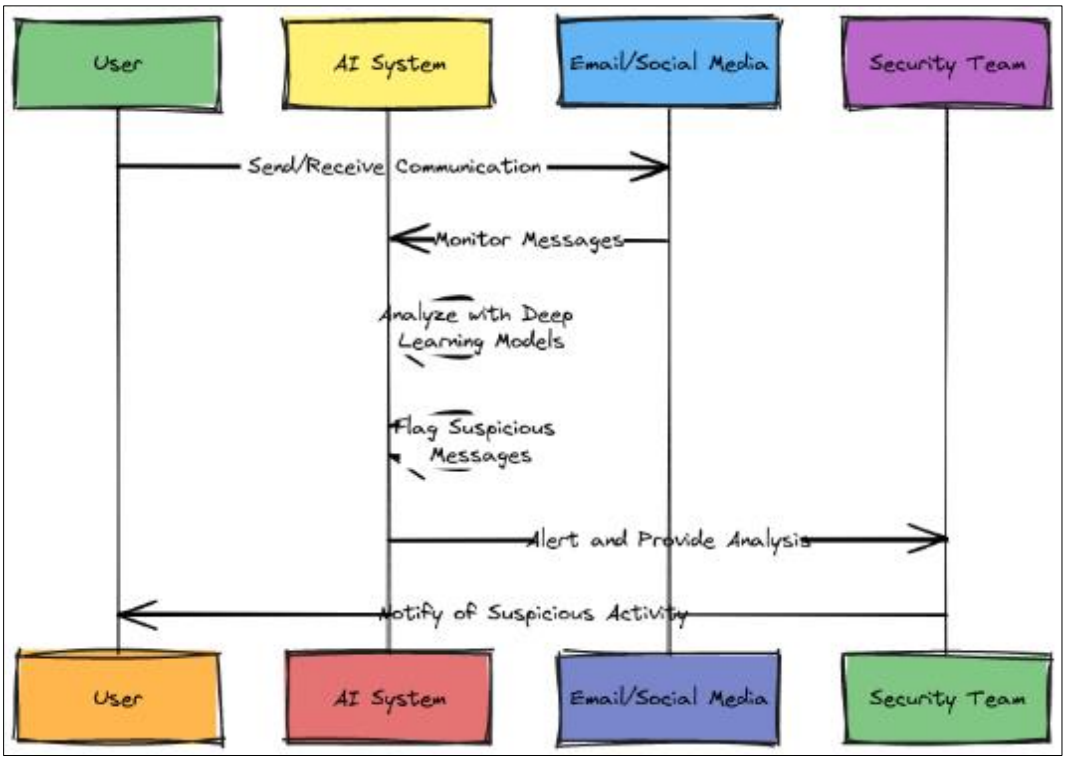

Figure 5 The role of AI in detecting social engineering attacks

4.7. Boosting Optimization

As discussed earlier, security personnel is a limited resource and are normally overburdened with the pure volume of alerts that require attention making incident response prioritization a gruesome task. AI cannot be perceived as a backfill for incident responders; however, it can be used for prioritization of the security incidents that occur. AI can

help simplify the work of security personnel by prioritizing security alerts which controls resource allocation by ensuring that threats with the greater risks are given higher priority.

Recognizing Cyberattack Trends: Many threat actors will place information regarding attacks against organizations within social media platforms. The capability of AI can be used to identify trends from social media in order to determine the popularity of different attacks across various business sectors as well as the attacks that cybersecurity professionals have categorized as the gravest concern [26]. Analysis at this level and scale is implausible for security personnel, but AI can assist companies with mining beneficial insights out of large quantities of data in order to identify cyberattack trends.

Artificial Intelligence for IT Operations (AIOps) Infrastructure: AIOps platform can be used by security personnel to procure a great amount of clarity around data security. These platforms can perform observation as well as directly combat threats [26]. AIOps can categorize large amounts of data originating from a variety of infrastructure components in order to identify threat actors regardless of behavioral attributes in different situations. Probable attacks can be identified and stopped before they become successful with an AI implementation that analyzes a large dataset encompassing both normal traffic as well as illegitimate traffic in order to forecast and mitigate threats prior to their occurrence.

Authentication using Biometrics Technology: Facial recognition systems used for authentication are becoming more dependable as software development teams are enhancing this capability using AI. Machine learning builds a model for biometric authentication using facial recognition centered around associations and blueprints. The strength of an AI-powered facial recognition system is that it remains competitively operational with facial hair growth, hairstyle alteration, donning an accessory such as a hat.

Access Control Management: Access control methods can be enhanced through AI integration. For instance, illicit behavior and abnormal sign-on requests can be located by machine learning in order to find possible security incidents. Also, password management can be augmented to recognize inadequate passwords and automatically instruct end users to improve the password quality.

Botnet Protection: Botnets can present a significant threat to an organization's systems through account hijacking, data fraud, and creating fake accounts. It is possible for AI and machine learning to craft a defense against botnets as they can be trained to identify malicious bots, real end-users, and good bots from the stream of online web traffic. This capability empowers cybersecurity personnel to understand the characteristics of malicious traffic in order to establish diligence and defensive mechanisms against illegitimate bot traffic [29].

Breach Risk Projection: An organization's technology asset inventory can be gathered and related to potential threats to determine the infrastructure components and applications that are at significant risk of attack and exposure. AI can provide awareness regarding weaknesses in an organization's infrastructure and applications so that appropriate tactical and strategic steps can be taken to improve security controls as well as processes. Performing this planning will allow an organization to better understand the overall threat landscape and align both security controls and staffing in an efficient manner ensuring that resources are allocated using appropriate prioritization.

Threat Response Exhaustion: Security personnel can experience exhaustion which may result in the manifestation of additional security issues if not addressed in an appropriate manner. This condition is often the result of an array of security controls transmitting a bombardment of alerts to the security teams requiring decisions to be made and actions to be performed [31]. AI can be used to prioritize the incoming alerts in order to streamline security operations ability to manage the threats in the most applicable way. In addition, machine learning can be enabled to take prudent action to manage certain types of alerts.

Minimization of Human Configuration Inaccuracies: One of the main causes of cybersecurity issues can be directly attributed to human error. There are multiple reasons for this including the layering of security controls and human fatigue given the need to manage patching and day-to-day administrative tasks [30]. Issues that manifest themselves as the infrastructure is renovated, adjusted, changed can be identified by tools with embedded AI. These tools can provide opportune guidance regarding issues that are identified to humans. Using this guidance, the cybersecurity teams can also procure mitigation alternatives or enable AI systems to alter configuration attributes to remediate the identified risk.

Automation of Repetitive Tasks for Human Efficiency: During security incidents requiring threat response, the extent of the threat can change swiftly. This rate of change may hinder human response given precipitous complications.

However, AI and machine learning are unfazed by any unanticipated change of direction and will respond without any interruption.

Threat Response Time: Threat actors have received a significant advantage from recent technological advancements which has resulted in attacks becoming more common as well as moving in a more expeditious fashion. Response from security operations can be delayed from the beginning of the incident which could lead to substantial amount of damage [32]. AI enabled security can collect information regarding the attack in order to organize the data and perform analysis and deliver a concise report. This provides quick recommendation for the security teams to take preventative measures to limit the damage caused and potentially stop similar attacks from occurring in the future.

Insider Threat Detection: Personnel who are allocated access to confidential data and further make use of this access to transfer since the sensitive information to users outside of the organization that are unauthorize to access the material are referred to as an "internal threat". Insider threats can be a crippling outcome for organizations, but AI offers the ability to identify and mitigate this risk. Through predictive and behavioral analysis, employees performing actions that are suspicious can be detected. In this way, AI can stop security incidents from occurring.

Cyber Threat Intelligence: Cyber threat intelligence stands to benefit from AI in several ways including the accumulation, manipulation, and examination of data. AI makes it possible to improve data curation in order to establish confirmation with additional providers. AI can further transform the cyber threat intelligence into a series of defensive steps that can be taken from strategic, tactical, and operational level of cybersecurity. Data can be collected from network security control applications by AI in order to compare this data to information available from elsewhere. It is expected that malware discovery will be enhanced by AI including the ability to classify different variants to an appropriate malware family by identifying some hidden attributes that are not noticed when humans examine the malware sample [16].

The following sequence diagram explains the flow of data from network security controls through AI processing leading to actionable cyber threat intelligence.

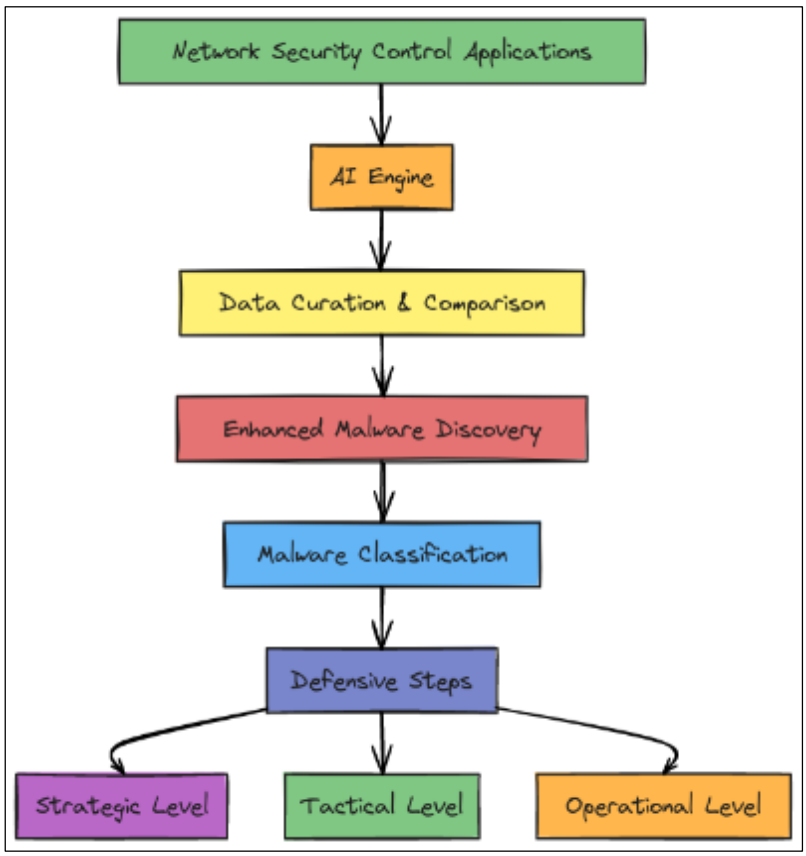

Figure 6 Cyber Threat Intelligence (CTI) using Artificial Intelligence

As the cybersecurity threats continue to advance, the requisite for innovative tools and tactics to protect against malicious attack vectors becomes more significant. The realm of AI has surfaced as an effective tool to aid in the detection, evaluation, and mitigation of cyber threats. AI also has the potential to transform the cybersecurity landscape by offering powerful tools for processes such as threat analysis, categorization of risks, remediation assistance, malware discovery, social engineering detection, utilizing AIOps IT infrastructure, extrapolation of breach risks, insider threat exposure, and cyber threat intelligence. By harnessing the power of AI, cybersecurity personnel can actively safeguard against the evolving and sophisticated landscape of cyber threats.

In order to assure that an organizations' sensitive and confidential information remains safe and secure, it is essential that the course of actions to counteract to cyberattacks are swift and efficient. Exhausting cybersecurity personnel to inspect enormous amounts of data and react to potential threats in real time is a laboriously challenging process [31]. AI can automate this instantaneously by filtering through staggering amounts of data and recognizing threats while handling this a mundane task. The process of organizing data certainly leads to the occurrence of false positives when the only factor of reliance is human expertise. AI can assist in probing and reducing threats by allowing more efficient resource distribution and decreasing the amount of required manpower.

Machine Learning is described as a series of artificial intelligence algorithms that can be used "learn" from vast amounts of known examples and behavioral blueprints of adversarial tactics and techniques. Machine learning algorithms can also examine massive amounts of information to detect archetypes and signatures related to known threats and categorize them in accordance. This methodology minimizes the time period required for manual threat identification freeing the time for cybersecurity personnel to respond to potential threats in a swift manner [30]. Risk analysis is another notable aspect of AI enhancing cybersecurity. This involves classifying potential vulnerabilities and calculating the likelihood and effect of different cyber threats. AI algorithms can explore data from different source origins including network and system security logs in order to find impending threats and assess the probability of future attacks. This helps organizations prioritize their cybersecurity efforts and allocate resources more effectively.

AI can be readily integrated into the IT infrastructure to create an AIOps environment which enables organizations to computerize and simplify various standard IT processes including surveillance, notification, and incident response in order to reduce the risk of cyberattacks resulting from operational errors [24]. AI can also be trained to detect different types of malware through behavioral analysis and anomaly detection by providing a sizeable and diverse datasets which are capable of gathering and studying multiple instances, flagging common patterns and characteristics thereby reducing the overhead contributing to the aftermath of a malware related security incident.

Convergence of AI capabilities and human expertise can lead towards comprehensive understanding of the current threat landscape and establishment of robust proactive measures to defend against active vulnerabilities and locate novel threats. However, it is critical to note that AI can be recognized as an auxiliary tool to complement and enhance human expertise and intervention for better decision-making abilities [17]. Only through an integrated approach can organizations achieve comprehensive cybersecurity protection.

List of Abbreviations

The table below provides an explanation for the abbreviations and acronyms used in the paper.

Acronym/Abbreviation	**Meaning**
ACL	Access Control List
AI	Artificial Intelligence
AIOps	Artificial Intelligence for IT Operations
IT	Information Technology
NLP	Natural Language Processing
SEG	Secure Email Gateway
SOC	Security Operations Centre

5. Conclusions

Organizations are being confronted with security concerns that are continuing to grow more complicated and ever-changing threat landscape combined with mounting attack surfaces. Organizations are turning to AI in order to assist with alleviating these challenges. AI is effectively a force multiplier that enhances the productivity of an organization's security personnel by utilizing automation in locations that provide the greatest value. Contemporary security controls can be rigorously affected by mundane attacks while AI integrated solutions can aid with the resolution of this problem in order to fight against the threat actors. Many of the current AI solutions target threat detection in order to obtain an advanced warning for new threats giving organizations time for cybersecurity preparedness. As there are many use cases of AI in cybersecurity, an organization has to determine the best integration points for this game-changing technology. In order to do so, an organization must establish a strategic plan for the deployment of AI based on several different factors including applications, infrastructure, policies, deficiencies in skilled workforce, and information. By planning out the deployment of AI, organizations can create a cohesive strategy that will mitigate significant security challenges while averting a variety of attack types. There are variety of use cases for AI that can provide a wide range of defensive capabilities for many different cybersecurity threats. Blending automation with AI unburdens security personnel to address higher priority security issues including zero-day attacks and hunting threats. AI will meet four key goals of most organizations including the reduction of noise, the reduction of time required for triage, accelerating investigations, and providing additional background regarding security control enhancement proposals. AI also delivers numerous capabilities for detecting unusual behaviors through analysis and inspection. With the adoption of novel technologies by most organizations, AI is continually progressing in order to assist with providing security solutions to the latest threats in order to protect infrastructure and applications. In the future, AI enabled security controls are expected to grow past the capabilities of firewalls and anti-virus solutions into the cloud-based AI solutions that can be inserted on a router to extend the security to all infrastructure components. It is also predicted that AI will evolve and improve to continuously learn during various attack scenarios to adapt and improve making it extremely tough for adversaries to overcome the AI model as the training never concludes.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Murugesan S (2022). The AI-Cybersecurity Nexus: The Good and the Evil. IT Professional, 24(5), September 2022, pp. 4-8, https://doi.org/10.1109/mitp.2022.3205529, Accessed: July 21, 2024.

[2] Tolido R, Thieullent AL, Van der Linden G, Frank A, Delabarre L, Buvat J, Theisler, J, Cherian, S, & Khemka, Y (2019). Reinventing Cybersecurity with Artificial Intelligence. Capgemini. Available via https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf, Accessed: July 21, 2024.

[3] Muppidi S, Fisher L, and Parham G (2023). AI and Automation for Cybersecurity: How Leaders Succeed by Uniting Technology and Talent. IBM Institute for Business Value. Available via https://www.ibm.com/downloads/cas/9NGZA7GK, Accessed: July 21, 2024.

[4] Zeadally S, Adi E, Baig Z, & Khan IA (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access, vol. 8, pp. 23817-23837, https://doi.org/10.1109/ACCESS.2020.2968045.

[5] Zid B, Zid I, Lou X, and Waedt K (2023). Consideration of Artificial Intelligence for Cybersecurity Aspects of I&C Systems. ICONS-318, Feb. 2023. Available: https://conferences.iaea.org/event/181/contributions/15703/attachments/8560/11392/ICONS-318.pdf, Accessed: July 21, 2024.

[6] Fortinet (2020). Help Wanted: Next-generation AI for the Emerging Threat Landscape AI-based Threat Detection and Response Can Relieve Overwhelmed Security Staff While Mitigating Risk. FORTINET, Feb. 2020. Available via https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-next-generation-ai.pdf, Accessed: July 21, 2024.

[7] Iqbal A & Malik M (2023). Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. Available via

https://www.researchgate.net/publication/368821713_Deep_Learning_and_Artificial_Intelligence_Framework_to_Improve_the_Cyber_Security, Accessed: July 21, 2024.

[8] Bezombes P, Brunessaux S, & Cadzow S (2023). Cybersecurity of AI and Standardisation. ENISA, Mar. 2023. Available via https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation/@@download/fullReport, Accessed: July 21, 2024.

[9] Darraj E, Sample C, & Justice C (2019). Artificial Intelligence Cybersecurity Framework: Preparing for the Here and now With AI. European Conference on Cyber Warfare and Security, pp. 132-141,XIII, 2019. Available via https://www.proquest.com/conference-papers-proceedings/artificial-intelligence-cybersecurity-framework/docview/2261017088/se-2/, Accessed: July 21, 2024.

[10] Townsend K (2023). Cyber Insights 2023 | Artificial Intelligence. SecurityWeek. Available via https://www.securityweek.com/cyber-insights-2023-artificial-intelligence/, Accessed: July 21, 2024.

[11] Booz Allen Hamilton (2021). Cyber and AI: 2021 Technology Spotlight. Booz Allen. Available: https://www.boozallen.com/content/dam/boozallen_site/sig/pdf/white-paper/cyber-and-ai.pdf, Accessed: July 21, 2024.

[12] Johnson A & Grumbling Y (2019). Implications of Artificial Intelligence for Cybersecurity. National Academies Press, Washington DC, 2019. https://doi.org/10.17226/25488, Accessed: July 21, 2024.

[13] Krasser S, Kantchelian A, & Baggett D (2019). Currently Deployed Artificial Intelligence and Machine Learning Tools for Cyber Defense Operations. In 2019 Artificial Intelligence and Cybersecurity Operations at NAP.edu. National Academies Press, 2019, pp. 22-28. Available via https://nap.nationalacademies.org/read/25488/chapter/4, Accessed: July 21, 2024.

[14] PricewaterhouseCoopers (2023). Balancing Power and Protection: AI in Cybersecurity and Cybersecurity in AI - PwC Middle East. PwC. Available via https://www.pwc.com/m1/en/publications/documents/pwc-balancing-power-protection-ai-cybersecurity.pdf, Accessed: July 21, 2024.

[15] Sagar SB, Niranjan S, Kashyap N, & Sachin DN (2019). Providing Cyber Security using Artificial Intelligence – A survey. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, , pp. 717-720, https://doi.org/10.1109/ICCMC.2019.8819719, Accessed: July 21, 2024.

[16] Vähäkainu P, & Lehto M (2019). Artificial Intelligence in the Cyber Security Environment. ResearchGate. Dec. 2019. Available via https://www.researchgate.net/publication/338223306_Artificial_intelligence_in_the_cyber_security_environment_Artificial_intelligence_in_the_cyber_security_environment, Accessed: July 21, 2024.

[17] Belani G (2022). The Use of Artificial Intelligence in Cybersecurity: A Review. IEEE COMPUTER SOCIETY. Available via https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity/, Accessed: July 21, 2024.

[18] Columbus L (2019). 10 Ways AI And Machine Learning Are Improving Endpoint Security. Forbes. Available via https://www.forbes.com/sites/louiscolumbus/2019/09/25/10-ways-ai-and-machine-learning-are-improving-endpoint-security/?sh=4ca87ee62db0, Accessed: July 21, 2024.

[19] Sibanda I (2022). Why Artificial Intelligence Is the Future of Cybersecurity. Impact Networking. Available via https://www.impactmybiz.com/blog/ai-and-cybersecurity-future/, Accessed: July 21, 2024.

[20] The Hacker News (2023). How to Use AI in Cybersecurity and Avoid Being Trapped. The Hacker News. Available via https://thehackernews.com/2023/02/how-to-use-ai-in-cybersecurity-and.html/, Accessed: July 21, 2024.

[21] Korolov M (2022). Top Three Use Cases for AI in Cybersecurity. Data Center Knowledge. Available via https://www.datacenterknowledge.com/security/top-three-use-cases-ai-cybersecurity, Accessed: July 21, 2024.

[22] Holdeman E (2023). Cybersecurity: The Benefits and Threats of AI Technology. GovTech, Available via https://www.govtech.com/em/emergency-blogs/disaster-zone/cybersecurity-the-benefits-and-threats-of-ai-technology/, Accessed: July 21, 2024.

[23] Gray L (2021). 5 Interesting Applications of AI in Cyber Security in 2023. OnlineCourseing. Available via https://onlinecourseing.com/ai-on-security/, Accessed: July 21, 2024.

[24] Fortra's TS (2023). AI in Cyber Security: Pros and Cons | Terranova Security. terranovasecurity.com. Available via https://terranovasecurity.com/ai-in-cyber-security/, Accessed: July 21, 2024.

[25] Prakash M (2023). AI in Cyber Security: Use Cases, Advantages. www.knowledgehut.com. Available via https://www.knowledgehut.com/blog/security/ai-in-cyber-security/, Accessed: July 21, 2024.

[26] Columbus L (2023). Experts predict how AI will energize cybersecurity in 2023 and beyond. VentureBeat. Available via https://venturebeat.com/security/experts-predict-how-ai-will-energize-cybersecurity-in-2023-and-beyond/, Accessed: July 21, 2024.

[27] Kangas S (2022). Why AI is the key to developing cutting-edge cybersecurity?. World Economic Forum. Available via https://www.weforum.org/agenda/2022/07/why-ai-is-the-key-to-cutting-edge-cybersecurity/, Accessed: July 21, 2024.

[28] Newman J (2022). Artificial Intelligence in Cybersecurity: Use Cases & Future. www.itransition.com. Available via https://www.itransition.com/ai/cyber-security/, Accessed: July 21, 2024.

[29] Kaspersky (2020). AI and Machine Learning in Cybersecurity - How They Will Shape the Future. www.kaspersky.com. Available via https://www.kaspersky.com/resource-center/definitions/ai-cybersecurity/, Accessed: July 21, 2024.

[30] Joshi K (2022). How AI is Changing Cybersecurity: New Threats & Opportunities. Emeritus Online Courses. Available via https://emeritus.org/blog/cybersecurity-how-ai-is-changing-cybersecurity/, Accessed: July 21, 2024.

[31] BlackBerry (2023). Artificial Intelligence (AI) for Cybersecurity. www.blackberry.com. Available via https://www.blackberry.com/us/en/solutions/endpoint-security/cybersecurity-ai#kinds/, Accessed: July 21, 2024.

[32] Ravichandran H (2023). Council Post: How AI Is Disrupting And Transforming The Cybersecurity Landscape. Forbes. Available via https://www.forbes.com/sites/forbestechcouncil/2023/03/15/how-ai-is-disrupting-and-transforming-the-cybersecurity-landscape/?sh=278f0b064683/, Accessed: July 21, 2024.

[33] Rathnayake D (2022). Artificial Intelligence, a new chapter for Cybersecurity?. TripWire. Available via https://www.tripwire.com/state-of-security/artificial-intelligence-new-chapter-cybersecurity/, Accessed: July 21, 2024.