The Influence of AI's brain on Cybersecurity

Pyla Srinivasa Rao[1]
Senior Manager, Cyber Security, Capgemini,
India

T. Gopi Krishna[2], Teklu Urgessa[3]
[2,3]Department of Computer Science and Engineering,
School of Electrical Engineering and Computing,
Adama, Ethiopia

Abstract:- The adoption of Artificial Intelligence (AI) promises significant benefits to various domains, and one that stands out prominently is the field of Cybersecurity. Traditional system approaches, while commendable for their established track record, often prove sluggish and insufficient due to their lack of adaptability and intelligence. Cybersecurity is a significant concept in protecting different types of data in organizations. However, effective implementation is enhanced by using Artificial Intelligence to improve security. The integration of intelligent algorithms into cybersecurity practices has significantly enhanced the ability to detect and analyze malicious activities within computer networks. As the frequency and sophistication of cyberattacks continue to rise, there is a growing urgency to implement advanced security measures. Among the most promising technologies in the field of cybersecurity is artificial intelligence (AI), renowned for its capacity to identify threats and execute real-time automated responses. This article focused into the dual effects of AI on cybersecurity, exploring both its beneficial and detrimental aspects and this study has established three research objectives. 1) How is AI Utilized in the Field of Cybersecurity, 2) Does AI Represent the Future of Cybersecurity, 3) Why is AI Important in the Field of Cybersecurity. We conducted a comprehensive review of these objectives and deliberated on potential research questions.

Keywords:- *Cybersecurity; AI; ML; DL; Threats;Attacks.*

I. INTRODUCTION

Artificial intelligence has the potential to enhance security, but it can also grant cybercriminals access to systems without requiring human intervention. Artificial intelligence serves as both a blessing and a curse for customers, businesses, and cybercriminals alike. The adoption of Artificial Intelligence (AI) holds great promise across various domains, and one domain that particularly stands out is the realm of Cybersecurity. While traditional approaches to system security have a commendable track record, they often fall short in terms of adaptability and intelligence. Cybersecurity plays a vital role in safeguarding diverse types of organizational data. However, the effective fortification of these digital fortresses can be significantly bolstered through the integration of Artificial Intelligence. By infusing intelligent algorithms into cybersecurity practices, the capability to swiftly identify and scrutinize malicious activities within computer networks has been dramatically augmented.

Modern security teams encounter numerous obstacles, including advanced attackers, an ever-expanding attack surface, an overwhelming influx of data, and escalating infrastructure complexity, all of which impede their capacity to protect data, oversee user access, and promptly identify and counter threats. In an era marked by the escalating frequency and sophistication of cyberattacks, the imperative for advanced security measures has never been more pronounced. At the forefront of these measures lies artificial intelligence (AI), celebrated for its prowess in threat identification and real-time automated responses. AI can strike a balance between security and user experience by assessing the risk associated with every login attempt, confirming users through behavioral data, streamlining access for verified users, and slashing fraud costs by as much as 90%. This article discusses deep into the dual-sided impact of AI's brain effects on cybersecurity, meticulously exploring both its advantageous and potentially adverse effects. AI and machine learning have gained increasing prominence in the realm of cybersecurity, playing a pivotal role in the detection and mitigation of cyber threats. One notable application of AI is the identification of vulnerabilities within network traffic. Through the analysis of patterns in network data, AI systems have the capacity to pinpoint potential threats and promptly alert cybersecurity professionals [1, 2, 26].

Furthermore, AI's ability to analyze vast datasets is invaluable in uncovering threats that might elude human analysts initially. This capability proves particularly beneficial in identifying subtle and non-obvious threats.

AI also contributes to cybersecurity by automating routine tasks, reducing their time consumption. For instance, AI systems can automatically handle system patching and updates, liberating cybersecurity professionals to engage in more intricate responsibilities.

Additionally, AI aids in generating reports and alerts, furnishing invaluable insights that inform strategic cybersecurity decisions.

The potential advantages of AI in cybersecurity are substantial. By enhancing the speed and precision of threat detection and response, AI helps mitigate the impact of cyberattacks. It also streamlines cybersecurity operations, freeing up precious time and resources for other critical tasks.

➢ *Areas of Research Needs:*

The subsequent list, while not exhaustive, outlines the research gaps uncovered in our study.

- Crafting efficient AI models using a limited dataset, transitioning from big data to a small data environment.
- Expanding on the use of raw data to create end-to-end solutions, minimizing or even eliminating the need for extensive feature engineering and domain expertise.
- Integrating change detection and adaptation mechanisms to address non-stationarities, specifically changes in the time variance of system states.
- Regularly evaluating the validity of developed models to promptly identify and rectify potential biases that could introduce additional vulnerabilities.
- Developing strategies to eliminate existing biases, imbalances, and other factors that may degrade model performance.
- Establishing standardized datasets that adhere to these requirements, facilitating the reproducibility and comparison of AI-based solutions.
- Developing methodologies to differentiate between malicious attacks and system faults.
- Investigating the impact of an increased system scale, this affects the accuracy and computational complexity of AI-based tools and methodologies, thereby influencing their performance in the face of cyberattacks.
- Modeling interdependencies within cyber-physical systems to assess the consequences of vulnerabilities.
- Establishing a standardized performance evaluation framework to facilitate reliable comparisons between solutions addressing similar problems.
- Enhancing context awareness within machine learning to bolster resiliency.
- Integrating human involvement, such as training practitioners through real-world scenarios.

These research gaps, while pertinent to AI in general, hold particular significance in the context of cybersecurity applications.

➢ *Research Requirements:*

- Establishing test beds for the examination and enhancement of the performance of ML-based tools and technologies in cybersecurity.
- Creating penetration testing tools rooted in AI and ML to identify and exploit security vulnerabilities for evaluating attackers' behavior.
- Formulating standardized frameworks for assessing the preservation of privacy and information confidentiality, both in data flows and within the designed systems.
- Crafting AI training models tailored for practitioners, incorporating real-world scenarios.
- Establishing an observatory dedicated to monitoring AI and cybersecurity threats.

II. THE CONTRIBUTION OF ARTIFICIAL INTELLIGENCE TO CYBERSECURITY

A. Security Threat Identification and Reaction, Risk Management and Enhancing Compliance

AI is rapidly emerging as a crucial tool in the battle against cyberattacks. By enhancing the swiftness and precision of threat detection and incident response, AI has the potential to mitigate the impact of cyberattacks and malicious activities while also boosting the efficiency of cybersecurity operations. Nevertheless, the integration of AI in cybersecurity comes with its fair share of challenges and risks. As cybercriminals hone their AI-based attack techniques, it may trigger an ongoing "arms race" between cybersecurity experts and malicious actors. Responsible and ethical AI utilization is paramount, demanding appropriate oversight and the inclusion of human intelligence in decision-making processes. To ensure the responsible and effective application of AI in cybersecurity, businesses and organizations should collaborate with experienced cybersecurity professionals adept in AI systems [3,4].

Furthermore, robust policies and procedures must be in place to govern AI usage in cybersecurity. These may encompass guidelines and policies on AI system training, decision-making protocols, and bias prevention.

Lastly, staying abreast of the latest developments in AI and cybersecurity is essential. As AI technology continues to evolve, so too will the associated threats and opportunities. By remaining informed and adaptable, businesses and organizations can harness the advantages and maintain a proactive stance in safeguarding their interests.

B. Security Threat Identification and Reaction

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

C. Anticipating Breach Risks

AI systems play a pivotal role in establishing a comprehensive IT asset inventory, meticulously documenting all devices, users, and applications, each with varying levels of access to different systems.Leveraging this asset inventory in conjunction with threat exposure, as previously discussed, AI-based systems excel at forecasting potential points of compromise, enabling strategic resource allocation to bolster areas of heightened vulnerability.

Moreover, the prescriptive insights derived from AI-driven analysis empower organizations to fine-tune and enhance controls and processes, fortifying their cybersecurity resilience.

III. THE BENEFITS OF ARTIFICIAL INTELLIGENCE IN THE FIELD OF CYBERSECURITY

The Capgemini Research Institute conducted an analysis on the role of AI in cybersecurity, and their report, titled *'Revolutionizing Cybersecurity through Artificial Intelligence*,' emphatically underscores the pressing need for modern enterprises to fortify their cybersecurity defenses with AI..

As networks expand in size and data complexity increases, AI offers superior solutions for an organization's cybersecurity requirements. Put simply, the escalating complexities are beyond human capacity to manage independently, making the adoption of AI an inevitable necessity sooner or later [5].

A. Identifying Emerging Threats

AI offers the capability to detect cyber threats and potentially malicious activities, addressing the limitation of traditional software systems in keeping up with the constantly evolving landscape of new malware. Through the utilization of advanced algorithms, AI systems undergo training to identify malware, perform pattern recognition, and discern even the subtlest indicators of malware or ransomware attacks before they infiltrate the system [5]

Moreover, AI leverages its natural language processing capabilities to autonomously gather information by scouring articles, news reports, and research on cyber threats. This facilitates the acquisition of intelligence on emerging anomalies, cyberattacks, and preventive strategies, as cybercriminal tactics continuously evolve [5].

AI-based cybersecurity systems provide access to the latest insights on global and industry-specific threats, enabling organizations to make informed prioritization decisions. These decisions are based not only on potential attack vectors but also on the likelihood of specific methods being employed in cyberattacks [5].

B. Enhanced Precision and Effectivenes

AI-driven cybersecurity systems offer superior precision and efficiency in contrast to conventional security measures. As an illustration, AI can swiftly assess numerous devices for potential vulnerabilities, completing the task in a fraction of the time required by human operators. Moreover, AI algorithms excel in identifying intricate patterns that might prove challenging for human observation, resulting in a heightened level of accuracy when detecting malicious activities.

C. Enhanced Scalability and Economic Benefits

AI has the capability to automate labor-intensive security tasks, liberating valuable resources that can be redirected towards other critical aspects of your business. Furthermore, it possesses the ability to rapidly and precisely analyze extensive datasets, enabling the identification of threats far more swiftly than human counterparts. This results in reduced response times to security incidents and contributes to cost savings in the realm of cybersecurity defense. AI-powered tools excel in recognizing malicious activity by establishing correlations between diverse data points, facilitating proactive system protection. What's more, these solutions offer seamless scalability, allowing you to expand your protection measures without incurring substantial expenditures on hardware or additional personnel.

D. Artificial Intelligence's Proficiency with Extensive Data Sets

Artificial intelligence plays a pivotal role in uncovering concealed threats camouflaged within ordinary activities, making it an invaluable solution. Its automated capabilities enable it to sift through vast data volumes and scrutinize network traffic comprehensively to identify potential threats. This advanced technology is particularly beneficial when integrated with residential proxies, facilitating efficient data transfer. Furthermore, it excels in threat detection, swiftly identifying any potential risks within the network traffic [5].

E. Enhanced Vulnerability Management with Artificial Intelligence

Artificial Intelligence operates with remarkable speed, enabling rapid system assessments surpassing the capabilities of cybersecurity personnel. Consequently, it significantly reduces their workload and enhances problem-solving capabilities manifold. By identifying vulnerabilities within computer systems and corporate networks, AI empowers businesses to prioritize critical security tasks. This proactive approach allows for timely vulnerability management and the safeguarding of business systems.

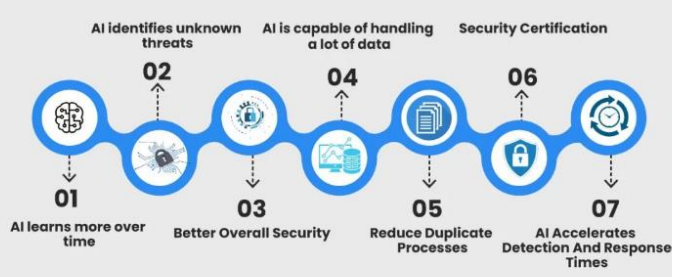

AI identifies unknown threats
AI is capable of handling a lot of data
Security Certification
02
04
06
01
AI learns more over time
03
Better Overall Security
05
Reduce Duplicate Processes
07
AI Accelerates Detection And Response Times

Fig. 1 Advantages of Employing AI in Cybersecurity

IV. DRAWBACKS OF AI IN THE FIELD OF CYBERSECURITY

The advantages highlighted earlier represent just a fraction of AI's potential to enhance cybersecurity. However, like any technology, there are drawbacks associated with the utilization of AI in this domain. Developing and maintaining an AI system necessitates substantial resources and financial investments. Moreover, AI systems rely on diverse datasets for training, encompassing numerous sets of malware codes, non-malicious codes, and anomalies. Accumulating these datasets is a time-consuming and costly endeavor, often exceeding the means of many organizations. In the absence of extensive data and event records, AI systems may yield erroneous results and trigger false positives. Relying on inaccurate data from unreliable sources can prove counterproductive. Additionally, a significant concern is that cybercriminals can harness AI to analyze their malware and orchestrate more sophisticated attacks, leading to the next point of consideration [10].

A. Inaccurate Alerts

One of the primary drawbacks associated with AI in cybersecurity is the risk of inaccurate alerts. AI-driven security systems depend on machine learning algorithms that derive insights from historical data. Nevertheless, this approach can produce inaccurate alerts when the system encounters novel, unfamiliar threats that deviate from established patterns. False positives have the potential to trigger alert fatigue, inundating security teams with a barrage of false alarms and potentially causing them to overlook legitimate threats.

B. The Shortage of Cybersecurity Expertise

Yet another drawback of AI in cybersecurity pertains to the prevailing skills gap within the industry. The operation of AI-driven security systems demands proficient experts capable of developing, deploying, and overseeing this technology. Regrettably, there is presently a scarcity of professionals possessing the requisite skills and expertise to effectively navigate AI in the realm of cybersecurity.

C. Cybercriminals Harness AI

Cybercriminals can employ AI to craft more sophisticated attacks and elude detection by AI-based security tools. Similarly, while neural fuzzing can aid in identifying vulnerabilities, it can also serve as a means for hackers to gather intelligence about the weaknesses of a target system.

Organizations must carefully assess both the advantages and drawbacks of AI in cybersecurity, striking a balance between the benefits and the associated costs and risks. The implementation of AI-powered security systems necessitates a comprehensive security strategy that incorporates additional technologies and human expertise to establish a multi-layered defense against evolving threats. In essence, while AI holds great promise within the cybersecurity domain, it is not a universal solution for all security challenges. Hence, organizations must maintain a vigilant and multifaceted approach to cybersecurity.

D. Expense

Deploying AI-driven security systems can incur significant expenses, particularly for smaller organizations operating within constrained budgets. The technology necessitates specialized hardware, software, and proficient professionals for both the development and maintenance of these systems.

E. Prejudice and Inequity in Decision-Making

Partial decision-making within AI systems can originate from diverse origins, such as datasets riddled with biased information or algorithms lacking requisite objectivity. When not effectively addressed, these biases can result in discriminatory judgments against specific groups or individuals, carrying substantial repercussions for the organization [7].

To illustrate, an AI system making decisions rooted in biased inputs might yield erroneous outcomes, obstructing genuine users from accessing company systems. This outcome could lead to diminished productivity or the loss of customers [6].

F. Absence of Clarity and Openness

The algorithms employed in security threat assessments don't always offer full transparency, potentially leaving vulnerabilities to bias or manipulation. AI systems can be intricate to decipher, rendering it challenging to discern the rationale behind decisions or ways to enhance them. This opacity can result in suboptimal choices, carrying significant consequences for an organization's security. AI-driven cybersecurity solutions may not consistently detect every threat or potential breach accurately, potentially allowing unnoticed risks to escalate and inflict additional harm.

G. Risk of Misapplication or Exploitation

The advantages of this technology are not exclusive to benevolent users. AI algorithms, with their capacity to swiftly sift through data and discern patterns, become an appealing target for malicious actors. They could potentially exploit these algorithms to access confidential information or launch attacks on critical infrastructure [11,26,27].

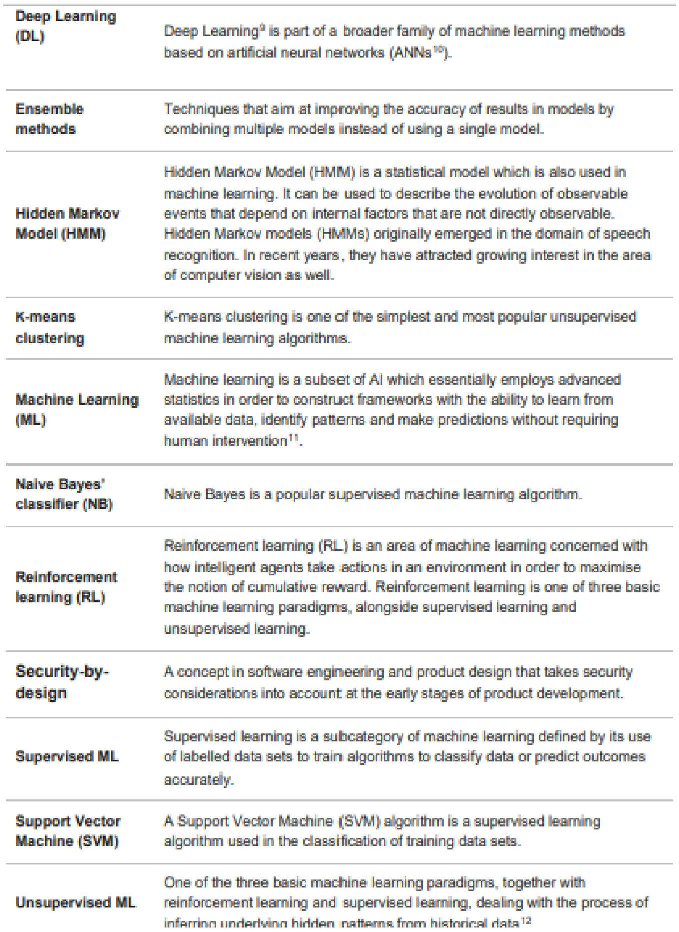
H. Examples of AI in Cyber Crime

Cybercriminals can employ AI for various nefarious purposes, including:

- *Effortlessly Crafting New Malware:* Utilizing AI to generate fresh malware with potential zero-day vulnerabilities or evasion tactics, which can bypass conventional detection methods.
- *Devising Sophisticated Phishing Attacks:* Crafting novel, sophisticated, and highly targeted phishing schemes to diversify attack scenarios, thereby challenging reputation engines to keep pace.
- *Rapid Data Analysis:* Harnessing AI's speed in data analysis to swiftly gather information and uncover additional attack vectors.
- *Generating Convincing Deepfakes:* Producing convincing video or audio deepfakes to deceive victims in social engineering attacks.
- *Executing Intrusions and Developing Hacking Tools:* Employing AI to execute intrusions and formulate new hacking tools.

Furthermore, AI's reliance on potentially biased or incomplete datasets can result in missed threats and false positives, fostering a deceptive sense of security that may lead to real-world consequences. Table 1. Shows the research techniques used of AI in cybersecurity.

TABLE I. AI AND CYBERSECURITY RESEARCH



Deep Learning (DL)	Deep Learning[9] is part of a broader family of machine learning methods based on artificial neural networks (ANNs[10]).
Ensemble methods	Techniques that aim at improving the accuracy of results in models by combining multiple models instead of using a single model.
Hidden Markov Model (HMM)	Hidden Markov Model (HMM) is a statistical model which is also used in machine learning. It can be used to describe the evolution of observable events that depend on internal factors that are not directly observable. Hidden Markov models (HMMs) originally emerged in the domain of speech recognition. In recent years, they have attracted growing interest in the area of computer vision as well.
K-means clustering	K-means clustering is one of the simplest and most popular unsupervised machine learning algorithms.
Machine Learning (ML)	Machine learning is a subset of AI which essentially employs advanced statistics in order to construct frameworks with the ability to learn from available data, identify patterns and make predictions without requiring human intervention[11].
Naive Bayes' classifier (NB)	Naive Bayes is a popular supervised machine learning algorithm.
Reinforcement learning (RL)	Reinforcement learning (RL) is an area of machine learning concerned with how intelligent agents take actions in an environment in order to maximise the notion of cumulative reward. Reinforcement learning is one of three basic machine learning paradigms, alongside supervised learning and unsupervised learning.
Security-by-design	A concept in software engineering and product design that takes security considerations into account at the early stages of product development.
Supervised ML	Supervised learning is a subcategory of machine learning defined by its use of labelled data sets to train algorithms to classify data or predict outcomes accurately.
Support Vector Machine (SVM)	A Support Vector Machine (SVM) algorithm is a supervised learning algorithm used in the classification of training data sets.
Unsupervised ML	One of the three basic machine learning paradigms, together with reinforcement learning and supervised learning, dealing with the process of inferring underlying hidden patterns from historical data[12]

V. ESSENTIAL CONSIDERATIONS FOR IMPLEMENTING AI SOLUTIONS

When developing your own AI solution, several critical factors warrant consideration:

- ***Data Integrity:*** The quality of your dataset significantly impacts your AI solution's performance. Ensure your dataset is clean and well-annotated for effective model training.
- ***Choosing the Model:*** The choice of the right model and the architecture of your AI system are pivotal. Selection depends on your specific problem, available data volume, and desired accuracy level.
- ***Hardware:*** Assess the computational demands of your AI solution and confirm that you possess the requisite hardware resources to support it.
- ***Transparency:*** As AI models grow in complexity, comprehending their decision-making processes becomes challenging. Prioritize the explainability of your model, particularly in sensitive domains like healthcare and finance.
- ***Data Security and Privacy:*** Safeguard both the data used for training and deployment and the system itself, taking into account security and privacy considerations.
- ***Growth Potential:*** Plan for the scalability of your AI solution, ensuring it can accommodate increased data volume or user numbers.
- ***Ethical Considerations*:** Reflect on the ethical ramifications of your AI solution, including bias and fairness.
- ***System Integration:*** Contemplate how your AI solution will seamlessly integrate with existing systems and workflows.
- ***Sustainment:*** Recognize that AI systems require regular maintenance and updates. Develop a strategy to ensure smooth, ongoing operation.
- ***Supervision:*** Establish protocols for monitoring your AI solution's performance and for identifying, troubleshooting, and rectifying issues that may arise.

VI. DEVELOPING AN EFFECTIVE AI STRATEGY FOR YOUR ORGANIZATION

Once you've formulated your AI strategy, it's essential to contemplate how and where to implement it most effectively. Since different organizations have unique cybersecurity needs, there's no one-size-fits-all approach. However, consider the following examples of how AI can be harnessed to educate and assist users in adopting best cybersecurity practices:[8,9,10]

- **Chatbots for Information and Guidance:** Organizations can introduce chatbots to furnish users with information and guidance on safeguarding their devices and personal data against cyber threats. These chatbots can also address queries about internal policies and procedures, offering swift and immediate responses without the need to raise help desk tickets or await human assistance.

- **Virtual Assistants for Device Setup:** For product vendors or when deploying new equipment to users, virtual assistants can offer step-by-step instructions on configuring and utilizing security features. This includes setting up firewalls, installing antivirus software, configuring security and privacy settings, managing sharing permissions, and more.

- **Cybersecurity Awareness Training:** Implement cybersecurity awareness training programs designed to educate users about common cyber threats and effective avoidance strategies. These programs can employ interactive simulations, quizzes, and practical exercises. Furthermore, machine learning can enhance these initiatives by leveraging evaluation results, quiz outcomes, surveys, cyber games and challenges, and phishing simulations to continually refine the training process [11.22.23,27].

When devising an implementation strategy, it's imperative to evaluate the potential risks inherent in AI-driven security tools and procedures. Conduct a thorough assessment of your existing infrastructure to pinpoint areas where AI can enhance performance, and assess the availability of relevant data for analysis.

Moreover, continuous evaluation of the efficacy of your AI security strategy is essential. This ongoing assessment enables you to ascertain whether your strategy aligns with its intended objectives and affords the flexibility to make necessary refinements.

VII. OPTIMAL APPROACHES FOR EMPLOYING AI IN CYBERSECURITY

AI holds the potential to revolutionize the cybersecurity domain. AI-driven technologies excel at identifying anomalies, scanning for vulnerabilities and malicious actions, and discerning patterns and behaviors indicative of potential threats. By harnessing AI's capabilities and adhering to best practices, you can enhance your cybersecurity stance and gain a competitive edge in the ever-evolving landscape of cyber threats.

Consider implementing the following best practices when integrating AI into your cybersecurity strategy:

- ***Establish Clear Objectives:*** Define precise goals for incorporating AI into your security efforts. This ensures efficient resource allocation and aligns technology implementation with your security objectives.

- ***Use High-Quality Data:*** Employ top-tier data for training AI models and verifying system-generated results. Poor-quality data can lead to inaccurate outcomes, including false positives or negatives, impacting overall system accuracy.

- ***Leverage Diverse AI Algorithms:*** Employ multiple AI algorithms to identify potential security threats, enhancing your ability to detect anomalies or malicious activities accurately. This enables timely threat identification and response.

- ***Continuous Monitoring:*** Routinely monitor the performance of your AI systems to ensure they meet expectations and provide precise results. This proactive approach helps identify potential issues and areas for enhancement.

VIII. THE EVOLVING LANDSCAPE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

The linchpin of safeguarding an organization's network resides in effective vulnerability management. In the relentless stream of daily threats, a company must initially detect them, categorize their nature, and then swiftly enact countermeasures to preempt any potential harm. The orchestration of comprehensive vulnerability management hinges upon an in-depth analysis and evaluation of available security measures. Here, AI research emerges as a formidable ally, offering invaluable insights and support.

Looking ahead, the fortification of organizational or systemic security could be significantly enhanced through the integration of artificial neural networks. These networks, over time, adeptly discern patterns and diligently scan for potential threats exhibiting analogous characteristics. Threats identified through this process are promptly thwarted. The synergy between artificial intelligence and cybersecurity creates a formidable barrier against hacking attempts, as AI continually refines its acumen by assimilating knowledge from diverse scenarios. This continuous learning curve renders hackers hard-pressed to outsmart the evolving intelligence of the system.

IX. CURRENT USES OF AI IN CYBERSECURITY

Numerous organizations are presently in the exploratory phase, delving into the potential applications of AI in cybersecurity.

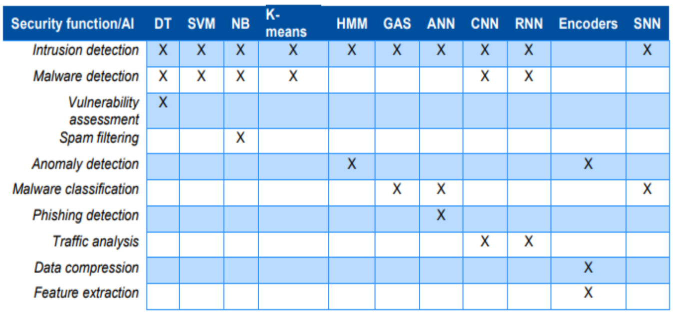
In sectors like banking and financial services, AI has already proven its worth, particularly in the realm of money laundering detection. Manual monitoring of millions of daily transactions for money laundering, while simultaneously considering all relevant regulations, is an insurmountable task for humans alone. However, AI models empower organizations to unearth previously concealed patterns and conduct extensive surveillance for suspicious activities at a scale unimaginable to human operators. According to Vartanian, these machines excel at tracking trends and identifying suspicious behavior in ways that surpass human capabilities [12, 13, 14, 21, 26,27].

In essence, the impetus for organizations to invest in AI for cybersecurity hinges on two contrasting motives, as articulated by Clinton. Firstly, there's the apprehension of being left behind, propelling organizations to embrace new technologies to avoid falling behind their competitors, even if they might not be fully prepared for such adoption. Secondly, there's a sense of caution stemming from concerns about the unforeseen consequences that may arise from AI implementation.

While AI platforms continue to advance, there's a pressing need for enhancements in their decision-making capabilities. At present, organizations can initiate the process by evaluating the potential advantages of AI in bolstering cybersecurity efforts in relation to its broader impact on the business.

The following Table 2. Shown the AI methods in cybersecurity functions [15, 16,17,18,27].

TABLE II. AI METHODS IN CYBERSECURITY FUNCTIONS



Security function/AI	DT	SVM	NB	K-means	HMM	GAS	ANN	CNN	RNN	Encoders	SNN
Intrusion detection	X	X	X	X	X	X	X	X	X		X
Malware detection	X	X	X	X				X	X		
Vulnerability assessment	X										
Spam filtering			X								
Anomaly detection					X					X	
Malware classification						X	X				X
Phishing detection							X				
Traffic analysis								X	X		
Data compression										X	
Feature extraction										X	

X. AI METHODS IN CYBERSECURITY FUNCTIONS

This section provides an overview of the current state-of-the-art in the primary applications of AI, including both traditional, well-established methods and newer deep learning systems, within the realm of cybersecurity. It encompasses various facets of AI's role in meeting cybersecurity requirements, addressing both malevolent and virtuous aspects. Below is a non-exhaustive list of ways in which AI can be applied in cybersecurity:[19,20,21,26].

- Cybercriminals leveraging AI to enhance their operational efficiency.
- Employing AI-based security mechanisms for the detection, identification, and mitigation of compromise-related consequences.
- Utilizing AI to exploit vulnerabilities within existing AI and non-AI tools and methodologies, such as adversarial attacks. Incorporating AI into system design to fortify existing AI and non-AI tools and methodologies as part of proactive protection measures during system development [24,25,26,27].

XI. CONCLUSION

For the average mid-sized startup or company, managing substantial network traffic is a daily challenge. The continuous flow of data between customers and the organization's servers necessitates robust protection against potential hacker threats. Safeguarding this data is vital to prevent both user and organizational harm, but the sheer volume of traffic makes manual monitoring by cybersecurity personnel impractical. Enter artificial intelligence (AI), a rapidly emerging innovation that is becoming a top priority for enhancing IT security teams' capabilities. Cybersecurity training programs, like Knowledge hut’s comprehensive offerings, equip cybersecurity professionals with a deep understanding of computer networks. The reality is that human resources alone cannot adequately secure an expansive attack surface at the enterprise level. AI offers critical analysis and threat identification capabilities that empower security experts to reduce breach risks and elevate overall security posture. Furthermore, AI aids in the identification and prioritization of risks, streamlines incident response, and detects malware attacks at an early stage, averting potential threats before they materialize. Despite the expected challenges, AI is poised to propel cybersecurity forward, enabling organizations to fortify their security posture effectively. For further insights and information, explore our resources. AI is fast emerging as a must-have technology for enhancing the performance of IT security teams. Humans can no longer scale to sufficiently secure an enterprise-level attack surface, and AI gives the much-needed analysis and threat identification that can be used by security professionals to minimize breach risk and enhance security posture. Moreover, AI can help discover and prioritize risks, direct incident response, and identify malware attacks before they come into the picture. So, even with the potential downsides, AI will serve to drive cybersecurity forward and help organizations create a more robust security posture [22,26,27].

ACKNOWLEDGMENT

We would like to thanks to Capgemini organization for providing research data and laboratory facilities in the real time.

REFERENCES

[1]. Bhardwaj, M.D. Alshehri, K. Kaushik, H.J. Alyamani, M. Kumar, Secure framework against cyber-attacks on cyber-physical robotic systems, J. Electron.
[2]. P. Chithaluru, A.T. Fadi, M. Kumar, T. Stephan, Computational intelligence inspired adaptive opportunistic clustering approach for industrial IoT networks, IEEE Internet Things J (2023), https://doi.org/10.1109/JIOT.2022.3231605.
[3]. I. Wiafe, F.N. Koranteng, E.N. Obeng, N. Assyne, A. Wiafe, S.R. Gulliver, Artificial intelligence for cybersecurity: a systematic mapping of literature, IEEE Access 8 (2020) 146598–146612..
[4]. I. Wiafe, F.N. Koranteng, E.N. Obeng, N. Assyne, A. Wiafe, S.R. Gulliver, Artificial intelligence for cybersecurity: a systematic mapping of literature, IEEE Access 8 (2020) 146598–146612.
[5]. Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, K.K.R. Choo, Artificial intelligence in cyber security: research advances, challenges, and opportunities, Artif. Intell. Rev. 55 (2022) 1029–1053..
[6]. J. Martínez Torres, C. Iglesias Comesana, ˜ P.J. García-Nieto, Machine learning techniques applied to cybersecurity, Int. J. Mach. Learn. Cybern. 10 (10) (2019) 2823–2836.M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.
[7]. Truong, I. Zelinka, J. Plucar, M. Candík, ˇ V. Sulc, ˇ Artificial intelligence and cybersecurity: past, presence, and future, in: Artificial intelligence and evolutionary computations in engineering systems, 2020, pp. 351–363.
[8]. V.G. Promyslov, K.V. Semenkov, A.S. Shumov, A clustering method of asset cybersecurity classification, IFAC-PapersOnLine 52 (13) (2019) 928–933.
[9]. V.L. Narasimhan, Using deep learning for assessing cybersecurity economic risks in virtual power plants, in: 2021 7th International Conference on Electrical Energy Systems (ICEES), 2021, pp. 530–537.
[10]. H.H. Nguyen, D.M. Nicol, estimating loss due to cyber-attack in the presence of uncertainty, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 361–369.
[11]. C. Ponsard, V. Ramon, M. Touzani, Improving cyber security risk assessment by combined use of i* and Infrastructure Models, in: the 14th International iStar Workshop, 2021, pp. 63–69.
[12]. P. Huff, K. McClanahan, T. Le, Q. Li, A recommender system for tracking vulnerabilities, in: The 16th International Conference on Availability, Reliability and Security, 2021, pp. 1–7.
[13]. Jian-hua LI, “Cyber security meets artificial intelligence: a survey,”. School of cybersecurity, Shanghai Jiao Tong University, Shanghai, China , 2018.
[14]. Lidestri, N., Maher, Stephen J., & Zunic, Nev.,” The Impact of Artificial Intelligence in Cybersecurity,”. ProQuest Dissertations and Theses, 2018.
[15]. 2021. S&T Artificial Intelligence and Machine Learning Strategic Plan. Technical Report. U.S. Department of Homeland Security.
[16]. Mohammed Almukaynizi, Eric Nunes, Krishna Dharaiya, Manoj Senguttuvan, Jana Shakarian, and Paulo Shakarian. 2017. Proactive identification of exploits in the wild through vulnerability mentions online. In Proceedings of the IEEE International Conference on Cyber Conflict US (CyCon US’17).

Institute of Electrical and Electronics Engineers Inc., 82–88.

[17]. Giovanni Apruzzese, Michele Colajanni, Luca Ferretti, Alessandro Guido, and Mirco Marchetti. 2018. On the effectiveness of machine and deep learning for cybersecurity. In Proceedings of the IEEE International Conference on Cyber Conflicts. 371–390.

[18]. S. Dilek, H. Çakır and M. Aydın,"APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING CYBER CRIMES: A REVIEW", International Journal of Artificial Intelligence & Applications (IJAIA), vol. 6, no. 1, 2015.

[19]. J.Raiyn, "A survey of Cyber Attack Detection Strategies", International Journal of Security and Its Applications, vol. 8, no. 1, pp. 247-256, 2014.

[20]. S. Simmons, D. Edwards, N. Wilde, J. Just and M. Satyanarayana, "Preventing Unauthorized Islanding: Cyber-Threat Analysis", 2006 IEEE/SMC International Conference on System of Systems Engineering, pp. 5, 24-26.

[21]. Artificial Intelligence Safety and Cybersecurity: A Timeline of AI Failures by Roman V. Yampolskiy and M. S. Spellchecker from https://arxiv.org/pdf/1610.07997.pdf.

[22]. Artificial Intelligence and its impact on Cyber Security from https://medium.com/@chiraghdewan/artificialintelligence-and-its-impact-on-cyber-security-1b2446d770b9.

[23]. The Risks of Artificial Intelligence to Security and the Future of Work Osonde A. Osoba, William Welser IV from https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237.pdf [22]. R. V. Yampolskiy, "Taxonomy of Pathways to Dangerous Artificial Intelligence," in Workshops at the Thirtieth AAAI Conference on Artificial Intelligence, 2016.

[24]. Kavak et al, 2021, Simulation for cybersecurity: state of the art and future directions, DOI: 10.1093/cybsec/tyab005, Oxford University Press (OUP), Journal of Cybersecurity.

[25]. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges, last access March 2023.

[26]. Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar. "Artificial intelligence for cybersecurity: Literature review and future research directions" , Information Fusion, 2023, https://www.sciencedirect.com/science/article/pii/S1566253523001136?via%3Dihub.

[27]. https://www.enisa.europa.eu.