STM JOURNALS

Journal of
Computer Technology & Applications

ISSN: 2229-6964 (Online)
ISSN: 2347-7229 (Print)
Volume 15, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoCTA

https://journals.stmjournals.com/jocta

Review JoCTA

Securing AI: A Survey Addressing Cyber Threats Arising in Cyber Security Due to Artificial Intelligence

S. Megha[1,*], Prasannakumaran K.S.[2]

Abstract

In today's ever-evolving technological landscape, the integration of Artificial Intelligence (AI) across various industries underscores the critical need for a robust cybersecurity framework. This comprehensive survey delves into the pressing necessity of safeguarding AI systems against cyber threats. Recent incidents have highlighted the alarming susceptibility of AI to malicious attacks, showcasing the potential repercussions of compromised systems. These attacks range from data manipulation to privacy infringements, posing significant risks to both individuals and organizations. This study delves into the intricate cybersecurity challenges facing AI, shedding light on common threats and their far-reaching consequences. Additionally, exploring the potential of AI itself to bolster cybersecurity measures, offering hope in the fight against malicious activities. By emphasizing the imperative of prioritizing cybersecurity in AI development and deployment, underscoring the importance of proactive measures to mitigate risks effectively. Ultimately, by acknowledging the dynamic nature of cyber threats and implementing robust defense mechanisms which can ensure the responsible and secure integration of AI into our society, safeguarding both technological advancements and user trust.

Keywords: Cybersecurity, artificial intelligence, cyber crime, safeguarding, cyber threats

INTRODUCTION

Motivation

Envision a future in which technology grows, learns, and changes with us, rather than just helping us. This is artificial intelligence's (AI) power; it is a revolutionary force that is reshaping the world today and tomorrow [1]. Artificial Intelligence is becoming a ubiquitous presence in our lives, facilitating ease, speed, and efficiency in everything from personalized recommendations on streaming services to life-saving medical diagnostics [2]. AI systems are becoming more and more essential in our daily lives as a result of handling enormous volumes of sensitive data. The necessity of preserving the integrity and security of these systems grows as AI develops.

***Author for Correspondence**
S. Megha
E-mail: smegha4321@gmail.com

[1]Student, Department of Computer Science and Engineering, College of engineering of Kallooppara, APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala, India
[2]Assistant professor, Department of Computer Science and Engineering, College of Engineering of Kallooppara, APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala, India

Received Date: June 26, 2024
Accepted Date: July 10, 2024
Published Date: July 26, 2024

Citation: S. Megha, Prasannakumaran K.S. Securing AI: A Survey Addressing Cyber Threats Arising in Cyber Security Due to Artificial Intelligence. Journal of Computer Technology & Applications. 2024; 15(2): 41–49p.

Problem Statement

Tremendous innovation also carries a high risk. The very interconnectivity and complexity that give AI systems their power also make them susceptible to cyberattacks [3]. Just picture the mayhem that would break out if these AI systems were breached. Potential repercussions of breaches in AI security include data leaks disclosing personal information, privacy violations affecting millions, and AI-driven choices altered with malevolent intent. In addition to embracing AI's potential, we must face the difficulties of protecting it from changing cyberthreats.

THE ROLE OF AI IN BOLSTERING CYBERSECURITY

The panorama of cyber threats is always changing, necessitating more advanced defenses. For organizations looking to strengthen their cybersecurity posture, artificial intelligence (AI) offers a potent tool. This is a thorough examination of how AI may support cybersecurity initiatives:

AI's Benefits for Cybersecurity

Improving Threat Detection and Prediction

- *Anomaly Detection:* AI is highly skilled in instantly evaluating enormous volumes of data to spot odd trends and departures from typical network behavior [4]. This makes it possible to identify possible cyberattacks, such as malware activities, dubious network traffic, or attempts at unauthorized access.
- *Threat Prediction:* To forecast upcoming cyberattacks, artificial intelligence (AI) algorithms can be trained on past data and attack trends [5]. Artificial intelligence (AI) can foresee possible dangers and proactively take preventative action by examining patterns and attacker behavior.

Streamlined Incident Response

- *Automated Response:* AI can initiate pre-programmed procedures to contain and lessen the impact of an attack when it detects a security threat [6]. This may entail alerting security personnel, quarantining compromised data, or isolating affected systems.
- *Better Decision-Making:* AI is capable of deciphering intricate security data and providing security analysts with useful insights. The amount of time and money required to look into and handle security incidents might be greatly decreased as a result [7].

Improved Security Evaluation

- *Vulnerability Assessment:* AI is capable of examining system configurations and software code to find possible weaknesses that an attacker could exploit [8]. By adopting a proactive approach, organizations can enhance their security measures and address vulnerabilities before adversaries have the opportunity to launch an attack.
- *Security Intelligence Gathering:* AI is capable of collecting and analyzing intelligence from a variety of sources, such as threat feeds, social media, and dark web monitoring, when it comes to security [9]. Security teams can stay up to date on new threats and attack techniques with the aid of this thorough overview of the cyber threat landscape.

LANDSCAPE OF AI AND ITS SECURITY CONCERNS

Types of AI

Based on its capabilities, functions, and technology, artificial intelligence can be roughly categorized into numerous forms. The three types of artificial intelligence and their related categories are depicted in Figure 1.

Based on Capabilities

a. *Weak AI:* Designed to perform specific tasks such as driving cars, conducting online searches, or recognizing faces [10]. Most AI systems in use today fall into this category, including those proficient in complex board games like Go and Chess. They operate within a limited, predefined scope.
b. *Strong AI:* This type of AI possesses advanced cognitive abilities comparable to humans, enabling it to independently tackle new and unfamiliar tasks. Such a powerful AI system could identify, learn from, and apply its knowledge to solve any problem without human assistance.
c. *Superintelligent AI:* This refers to a future scenario where machines surpass human intelligence in every intellectual domain, including creativity, general knowledge, and problem-solving. The idea of superintelligence is currently theoretical and has not yet been realized.

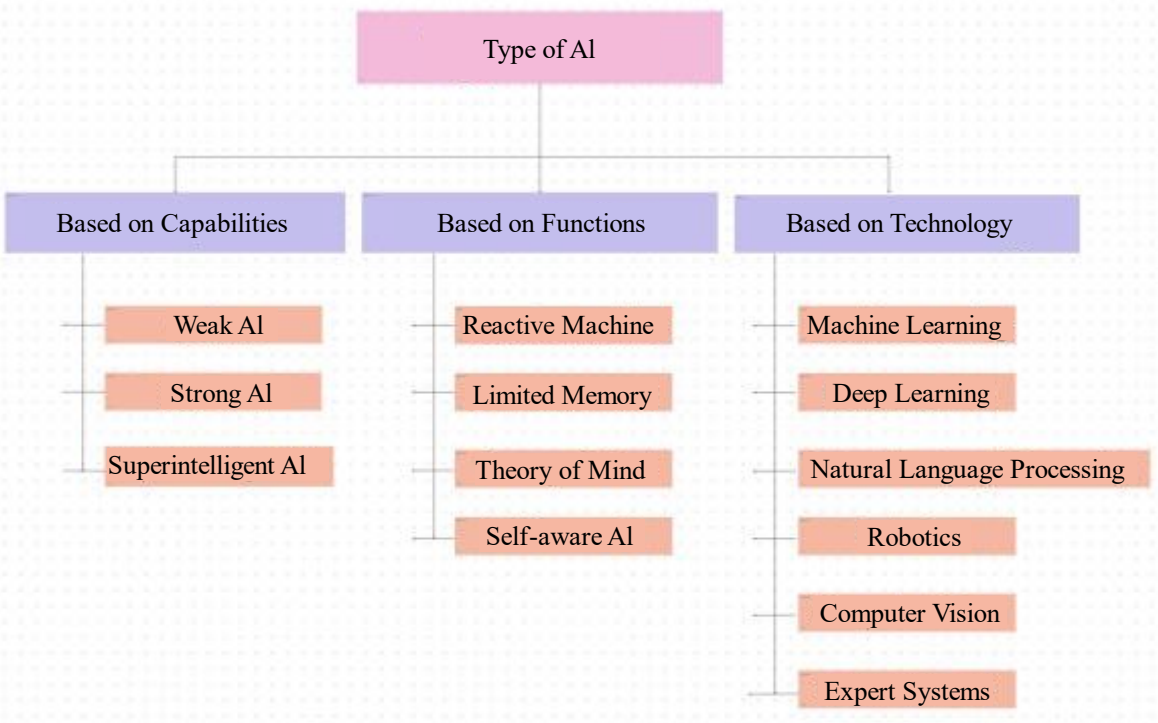

Figure 1. Types of AI.

Based on Functions

a. *Reactive Machine:* These AI systems do not store memories or past experiences for future use. They assess and react to various circumstances [11]. One example is IBM's Deep Blue, which defeated Garry Kasparov at chess.
b. *Limited Memory:* By examining the historical data that they have gathered, these AI systems are able to make better and more educated decisions. The majority of AI applications in use today, including self-driving cars and chatbots and virtual assistants, fit under this category.
c. *Theory of Mind:* Researchers are currently focusing on this more developed kind of artificial intelligence. It would include comprehending and keeping in mind needs, beliefs, and emotions in order to base decisions. For this kind, the machine must actually comprehend humans.
d. *Self-aware AI:* This is an example of AI in the future, where robots will be sentient, conscious, and self-aware. Although still in theory, this kind of AI may perceive and feel emotions, which could cause it to develop desires and beliefs.

Based on Technology

a. Machine Learning (ML): Algorithms can learn from data in this fundamental AI technique without the need for explicit programming [12]. There are several ML subfields, and each has advantages and disadvantages in terms of security:
    1. *Supervised Learning:* Labelled data, such as spam/non-spam emails, is used to train models. Applications for security include anomaly detection and virus detection.
    2. *Unsupervised Learning:* In unlabeled data, models identify patterns. One application of security is the detection of unusual network traffic patterns.
    3. *Reinforcement Learning:* In a simulated setting, models learn by making mistakes. AI firewalls are one example of a security application that may be trained to adapt to new attack techniques.
b. *Deep Learning (DL):* Deep Learning (DL) is a subset of machine learning that utilizes multi-layered artificial neural networks inspired by the structure of the human brain. DL might be opaque and complex, yet it is quite good at recognizing patterns. Image and speech recognition are used in security applications to detect threats, but they also pose privacy issues.

c. *Natural Language Processing (NLP):* Through natural language processing (NLP), computers are capable of understanding and processing human language. Applications for security include spotting phishing attempts and monitoring social media for indications of cyberattacks. Nevertheless, well written content has the potential to manipulate NLP models.
d. *Robotics:* This discipline involves information processing, sensory feedback, the design and construction of robots, their operation, and the use of computer systems for control.
e. *Computer Vision:* With the use of this technology, robots can now read visual cues from their environment [11]. It finds usage in a variety of fields, including manufacturing, medical image analysis, and surveillance.
f. *Expert Systems:* These AI systems use rule-based systems to provide answers to queries and resolve issues in a particular field of expertise.

Security Risks in AI

Industries are fast changing due to artificial intelligence (AI) technologies; nevertheless, as these systems become more complex, new security challenges arise. Due to their frequent handling of enormous volumes of sensitive data, these AI systems are susceptible to cyberattacks that could skew their results, steal personal data, or even cause them to make biased decisions. It is essential to comprehend and reduce these security threats in order to guarantee the ethical and reliable development and application of AI, since just like other technologies, AI systems are not immune to attacks. Here are a few common risks lurking in the shadows:

Data Driven Threats

a. *Data Poisoning:* When AI models are being built, malicious actors have the ability to alter the training data. This may entail introducing inaccurate or deceptive information into the data in order to distort the results of the model [13]. For instance, tampering with an image recognition system might cause self-driving cars to misread pedestrians or traffic signs.
b. *Data Leakage:* During the course of the AI development process or while the system is operating, sensitive information may unintentionally become public. This could include inadvertent information leaking through the model's outputs or data breaches that occur during transmission or storage.
c. *Privacy Concerns:* Effective operation of AI systems often requires vast amounts of data [14]. This poses privacy concerns for users, particularly when sensitive personal data is involved, such as financial or medical records. Additionally, by using strategies like model inversion, AI models may unintentionally pick up on and divulge sensitive information from training data.
d. *Data Bias:* The effectiveness of AI models hinges on the quality of the training data. The AI model will inherit the biases included in the training data and generate unfair or discriminatory results [15]. For instance, a resume screening engine driven by AI and educated on biased data may routinely minimize resumes from minorities or women.

Model-Specific Threats

a. *Model Hijacking:* This is taking unapproved control of an AI model in order to sway its judgement or produce undesirable results. To do this, attackers may take advantage of holes in the model's security settings or code [16]. A recommendation system that has been taken over may spread dangerous information or rig financial transactions.
b. *Model Inversion:* This describes methods that an attacker can use to extract private data from a trained artificial intelligence model. This data may compromise privacy since it contains personal information about specific people or events that were utilized to train the model.
c. *Adversarial Attacks:* An adversary may create particular inputs meant to trick artificial intelligence algorithms [17]. These inputs, which are frequently marginally altered copies of authentic data, may lead to inaccurate predictions from the model. An adversarial attack on a facial recognition system, for example, could include subtly altering an image's appearance to make it unrecognizable.
d. *Explainability Issues:* A lot of AI algorithms, particularly deep learning models, are intricate "black boxes". Understanding the rationale behind some of their judgments can be difficult. This

inexplicability makes it difficult to respond to security issues effectively and raises questions about accountability and justice [18]. For example, it could be difficult to determine and rectify potential bias if an AI loan approval system rejects a loan application and fails to provide a clear explanation for the refusal.

Systemic Threats

a. *Security Vulnerabilities in Development Tools:* Vulnerabilities that can be exploited can arise from defects in code libraries or development frameworks that are used to construct AI models [19]. These flaws might give attackers the ability to introduce malicious code, tamper with the training procedure, or obtain unauthorized access to private information.
b. *Physical Security Risks:* Artificial intelligence (AI) systems and the infrastructure that supports them may be susceptible to manipulation or tampering if proper physical security measures are not implemented. This might entail physically breaking into servers or other storage devices that hold AI models or data, therefore jeopardizing their integrity.
c. *Integration Risks:* The way AI technologies are coupled with other systems in an organization's network might lead to security flaws. An AI system linked to a crucial financial system, for instance, may have weak security measures, which could provide an opening for hackers.
d. *Supply Chain Risks:* When developing or implementing AI systems, third-party parts or services may bring vulnerabilities. These might be weaknesses in the hardware, software, or cloud platforms that the AI system uses.

Social and Societal Threats

a. *Job displacement:* AI automation has the capability to replace jobs in various industries as it advances. Even though there may be an increase in employment, the shift may be unsettling and result in unemployment and financial difficulties [20].
b. *Algorithmic Bias:* If AI systems are educated on biassed data, they may reinforce or magnify preexisting societal biases. Discriminatory outcomes in the criminal justice system, job decisions, and loan approval processes may result from this [21].
c. *Autonomous Weapons Systems:* The development and use of AI-driven autonomous weapons raise ethical and security concerns. International controls are necessary due to the possibility of unforeseen consequences or misuse of such weapons.
d. *Social Manipulation:* AI has the potential to be used maliciously to disseminate false information or sway public opinion. This could entail making up social media personas, producing convincing material, or sending targeted propaganda to specific people.

COUNTERMEASURES

Even though AI has many benefits for cybersecurity, its use has certain drawbacks that must be addressed. Below is a thorough analysis of the countermeasures being developed to lessen these difficulties:

Explainability

- *Explainable AI (XAI) Techniques:* XAI approaches are being actively developed by researchers to increase the transparency of AI models [22]:
    1. *Feature Attribution:* Techniques such as LIME (Local Interpretable Model-agnostic Explanations) offer an explanation of how particular data attributes influence a model's conclusion.
    2. *Trees of Decisions:* When opposed to intricate deep learning models, simpler rule-based models may be simpler to understand.

Bias

Techniques for detecting and mitigating bias in training data are being developed [20]. These include:

1. Data augmentation is the process of producing artificial data to compensate for underrepresented populations in the training set.

2. *Metrics for Fairness:* Metrics such as equal opportunity or statistical parity can be used to find and fix possible biases in the model's results.

Adversarial Attacks

- Adversarial training is the process of exposing AI models to adversarial cases in order to strengthen their resilience [23]. This helps the model to detect and defend against these covert attacks.
- *Group Techniques:* Creating diverse AI models with varying topologies might be a challenge to adversaries seeking to create effective hostile examples.

Additional Security Protocols

- A more complete defense can be achieved by implementing multi-layered security, which integrates AI with conventional security solutions like firewalls, intrusion detection/prevention systems (IDS/IPS), and vulnerability scanning.
- *Continuous Monitoring and Improvement:* Retraining AI models with new data and routinely assessing their performance for biases are essential to preserving their efficacy.

We can create AI-powered cybersecurity solutions that are more reliable and strong by implementing these countermeasures. Staying ahead of evolving cyber dangers is a continuous effort that requires cooperation between researchers, security experts, and policymakers.

FUTURE DIRECTION

Artificial Intelligence and cybersecurity is a field that is always changing and requires new strategies to keep ahead of cyberattacks. Here is a look at some fascinating future paths that prioritize proactive defense tactics, ongoing learning, and human-AI collaboration:

Human-AI Collaboration and Explainable AI (XAI)

- *Shifting Focus:* The importance of human expertise will always be recognized in the future of AI security. People and AI will increasingly work together to discover and analyze threats, with AI assisting with the analysis and threat identification while people use their contextual awareness and judgement to make crucial security decisions [24].
- *Enhanced Explainability:* As Explainable AI (XAI) methods advance, AI models will become easier to understand. This will encourage human-AI trust and cooperation. By understanding the reasoning behind AI decisions, security analysts will be better equipped to respond intelligently and increase the overall efficacy of security measures.

Threat Prediction and Proactive Defense Powered by AI

- *Advanced Threat Modelling:* Artificial intelligence will be utilized to develop complex threat models that take into account attacker behavior, psychology, and new trends in addition to past data [25]. As a result, we will be able to take a more proactive approach to cybersecurity and stop assaults before they start.
- *Autonomous Defense Systems:* Artificial intelligence (AI)-driven systems that can react autonomously to impending threats may be available in the future. This can entail conducting counterattacks to thwart ongoing cyberattacks, patching vulnerabilities, or even isolating infected systems. To avoid unexpected results, fail-safe features and ethical concerns would be essential in such systems.

Continuous Learning and Adaptation

- *Real-time Threat Analysis:* AI systems are designed to continuously learn from and react to real-time data sources [26]. This covers dark web analysis, social media monitoring, and threat intelligence reports. They are able to recognize novel attack vectors and modify their defenses as a result of their ongoing learning.

- *Adversarial Machine Learning:* The field of adversarial machine learning will be crucial as attackers create increasingly complex techniques to take advantage of AI weaknesses [27]. Here, AI will be utilized to generate adversarial scenarios in order to evaluate the resilience of AI security systems and find vulnerabilities before they can be taken advantage of by attackers.

Integration with Security Fabrics

- *Unified Security Ecosystem:* AI-powered security solutions will be easily incorporated into larger security fabrics, creating a unified security ecosystem [28]. This covers vulnerability scanners, firewalls, and intrusion detection/prevention systems (IDS/IPS). This all-encompassing strategy will offer a thorough understanding of the security environment and facilitate a better-coordinated defense.
- *Zero-Trust Security:* The term "zero trust" refers to the idea that all users and devices must be verified before access is allowed. When analyzing user behavior patterns and spotting anomalies that could be signs of insider threats or unauthorized access attempts, artificial intelligence (AI) can be quite helpful.

Security Considerations in the AI Development Lifecycle

- *Security by Design:* The whole AI development lifecycle, from design and training data selection to deployment and continuous monitoring, will incorporate security issues. This proactive strategy, will help reduce vulnerabilities from the start.
- *Formal Methods of Verification:* The accuracy and security characteristics of AI models will be mathematically proven by the application of formal verification techniques, a technique taken from software engineering. This can help identify any security vulnerabilities before AI systems are deployed in critical applications.

We can use AI's power to build a more secure and robust future for AI systems by investigating these potential directions. To keep ahead of the curve, cooperation between researchers, security experts, and legislators is necessary on this never-ending path.

CONCLUSION

The fields of cybersecurity and artificial intelligence are seeing rapid growth and change. Although AI has the potential to profoundly transform many aspects of our lives, safeguarding its development and deployment is essential.

This exploration has provided insight into our current situation and future goals. AI has proven to be a useful tool for cybersecurity, helping to predict potential threats and streamline incident response. But issues like bias and explainability demand constant attention.

Exciting opportunities lie ahead, with human-AI cooperation taking center stage. Think of AI as a vigilant watchdog that is always learning and changing, while security analysts use their knowledge to make wise choices. Developing proactive defense techniques and ongoing education will be essential to avoiding cyberattacks.

Robust cybersecurity protocols are essential to ensure the ethical advancement and deployment of artificial intelligence. We can work towards a future in which artificial intelligence (AI) both empowers us and keeps us safe from bad actors by emphasizing cooperation, adaptability, and a "security by design" strategy. The secret to creating a future filled with AI's promise in a secure setting is the collaborative work of researchers, security experts, and legislators.

REFERENCES

1. Naomi Haefner, Joakim Wincent, Vinit Parida, Oliver Gassmann. Artificial intelligence and innovation management: A review, framework, and research agenda. Technol Forecast Soc Change. 2021; 162: 120392. ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2020.120392.

2. Mahind Rupali, Amit Patil. A Review Paper on General Concepts of "Artificial Intelligence and Machine Learning. Int Adv Res J Sci Eng Technol (IARJSET). 2017; 4(4): 79–82. 10.17148/IARJSET/NCIARCSE.2017.22.
3. Global Risks Report. (2023). World Economic Forum. [Online]. Available from: https://www.weforum.org/publications/global-risks-report-2023/
4. Kumar PA, Selvakumar S. Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. Comput Commun. 2013 Feb 1; 36(3): 303–19.
5. Wang W, *et al*. Attention-based LSTM for anomaly detection in honeypots. IEEE Trans Ind Inform. 2019; 15(10): 5832–5841. (https://arxiv.org/abs/2107.05561)
6. Shaukat Dar Kamran, Luo Suhuai, Varadharajan Vijay, Hameed Ibrahim, Xu Min. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. IEEE Access. 2020; 8: 222310–222354. 10.1109/ACCESS.2020.3041951.
7. Alabadi M, Celik Y. Anomaly detection for cyber-security based on convolution neural network: A survey. In 2020 IEEE International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 2020 Jun 26; 1–14.
8. Chakraborty S, Krishna R, Ding Y, Ray B. Deep learning based vulnerability detection: Are we there yet? IEEE Trans Softw Eng. 2021 Jun 8; 48(9): 3280–96.
9. Alani MM. Big data in cybersecurity: a survey of applications and future trends. J Reliab Intell Environ. 2021 Jun; 7(2): 85–114.
10. Strelkova O. (2017). Three types of artificial intelligence. [Online]. https://www.ibm.com/blog/understanding-the-different-types-of-artificial-intelligence/
11. Mohri M, Rostamizadeh A, Talwalkar A. Foundations of machine learning. 2nd Edition, MIT press; 2018 Dec 25.
12. Biggio B, Nelson B, Laskov P. Poisoning attacks against support vector machines. arXiv preprint arXiv:1206.6389. 2012.
13. Pulido-Gaytan LB, Tchernykh A, Cortés-Mendoza JM, Babenko M, Radchenko G. A survey on privacy-preserving machine learning with fully homomorphic encryption. InLatin American High Performance Computing Conference. Cham: Springer International Publishing; 2020 Sep 2; 115–129.
14. Bolukbasi T, Chang KW, Zou J, Saligrama V, Kalai A. Man is to computer programmer as woman is to homemaker? Debiasing word embeddings [preprint]. arXiv.org; 2016. Available from: https://arxiv.org/abs/1607.06520. DOI: 10.48550/arXiv.1607.06520.
15. Chang CL, Hung JL, Tien CW, Tien CW, Kuo SY. Evaluating robustness of ai models against adversarial attacks. In Proceedings of the 1st ACM Workshop on Security and Privacy on Artificial Intelligence. 2020 Oct 6; 47–54.
16. Goodfellow IJ, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572. 2014 Dec 20.
17. Lundberg S, Lee SI. A unified approach to interpreting model predictions [preprint]. arXiv.org; 2017. Available from: https://arxiv.org/abs/1705.07874. DOI: 10.48550/arXiv.1705.07874.
18. Frey CB, Osborne MA. The future of employment: How susceptible are jobs to computerisation? Technol Forecast Soc Change. 2017 Jan 1; 114: 254–80.
19. Si Zihua, Han Xueran, Zhang Xiao, Xu Jun, Yin Yue, Song Yang, Wen Ji-Rong. A Model-Agnostic Causal Learning Framework for Recommendation using Search Data. WWW '22: Proceedings of the ACM Web Conference. 2022; 224–233. 10.1145/3485447.3511951.
20. Das A, Rad P. Opportunities and challenges in explainable artificial intelligence (xai): A survey. arXiv preprint arXiv:2006.11371. 2020.
21. Biggio Battista, Roli Fabio. Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning. Pattern Recognit. 2017; 84: 317–331. 10.1016/j.patcog.2018.07.023.
22. Wirkuttis N, Klein H. Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security. 2017 Jan; 1(1): 103–19.
23. Mauri L, Damiani E. Modeling threats to AI-ML systems using STRIDE. Sensors. 2022 Sep 3; 22(17): 6662.

24. Fahim Sufi. A global cyber-threat intelligence system with artificial intelligence and convolutional neural network. Decis Anal J. 2023; 9: 100364. ISSN 2772-6622, https://doi.org/10.1016/j.dajour.2023.100364.
25. Biggio B, Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018 Oct; 2154–2156.
26. Paloalto networks. (2023). Gartner 2023 Magic Quadrant for SD-WAN. [Online]. Paloaltonetworks.com. Available from: https://start.paloaltonetworks.com/gartner-sd-wan-mq-2023.html?utm_source=google-jg-japac-sase-smco-wanm&utm_medium=paid_search&utm_campaign=google-sase-sdwan-japac-in-lead_gen-en&utm_content=7014u0000017kvYAAQ&utm_term=palo%20alto%20sd%20wan&cq_plac=&cq_net=g&gad_source=1&gclid=CjwKCAjw4ri0BhAvEiwA8oo6FwnXcA8IKwZ4fcrq9EZaNPkotkeIqAlzFHQ6Fgzo8URJUTN0lMnD9BoC0uQQAvD_BwE
27. Paloalto networks. (2021). The Evolution of ZTNA to Fully Support Zero Trust Strategies. [Online]. Paloaltonetworks.com. Available from: https://start.paloaltonetworks.com/the-evolution-of-ZTNA?utm_source=google-jg-japac-sase-smco-syhw&utm_medium=paid_search&utm_campaign=google-sase-shw-japac-in-lead_gen-en-eg-brand&utm_content=7014u000001kapoAAA&utm_term=palo%20alto%20prisma&cq_plac=&cq_net=g&gad_source=1&gclid=CjwKCAjw4ri0BhAvEiwA8oo6FwLI9YHHidDx5VYblO0FM-owIM160JSapeigKqJmkvgQQ4F-1eceoxoCev4QAvD_BwE
28. CISA. Principles and approaches for secure by design software. [Online]. Available from: https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf

