IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205226 |

The Paradoxical Situation: AI's Duelling Roles in Cyber Security

Monika, Dr. Febin Prakash

PG Student, School of Computer Science and Information Technology, Jain (Deemed-to-be University)

Bangalore, India

Asst. Professor, School of Computer Science and Information Technology, Jain (Deemed-to-be University)

Bangalore, India

ABSTRACT: With the emerging technology and devices, and humans stepping towards the advancements of technology with various advantages, it sounds good to know about the expansion, but there come the cons with pros of how the internet-connected device can manipulate privacy when humans become negligent towards their responsibility of how and what contents they are sharing on the internet, and at major, the lack of education of cybersecurity leads towards data breach. As the technology grows towards the upper edge and the development of AI and ML in every field, it has also become important to know how AI plays a role in cybersecurity and to know whether the step towards this path will lead to true sustenance. This paper is an acquaintance of AI, cybersecurity, and the relationship between them.

KEYWORDS: Cybersecurity, Artificial Intelligence, Challenges faced by AI

I. INTRODUCTION

The essence of modern artificial intelligence lies in its inherent paradoxes. On one hand, AI is designed to streamline automation, yet it paradoxically demands deeper human engagement to contemplate the insights it generates. This article delves into yet another contradiction: the dual nature of computational systems powered by AI. These systems can serve the public good in civilian applications, yet also harbor the potential for harm across various domains and settings. As we know and have seen, AI proves itself a superior "watcher" and "seeker" compared to a human agent, constantly vigilant for anomalies within a network and capable of autonomously selecting optimal responses. However, AI is not without its vulnerabilities. Like any computing system, it is susceptible to similar attacks, and unforeseen deviations can nullify its effectiveness, potentially lulling security analysts into a misleading sense of safety. From a short survey, it can be noticed that AI has boomed up due to its advantageous weight and success in almost all fields[1], but it is also to be noticed that any technology can be used for both good and evil based on the ethics of any individual or community, as its already known AI makes work autonomous the same applies here that it can be used for any purpose of good or bad, its not only about how AI can be manipulated by humans but also at some extent when human finally make Robots that pass the Turing test and can act as humans. There again comes a consequence, human behaviour also have negative sides, which may be incorporated into machines ,by humans mistakenly, there have been many cases that have to be considered where AI has misguided goals[1]which makes it more dangerous when AI does not need any human support to support itself, that is AI becoming self-dependent. The further paper contains basic information on each of the relevant topics and how it's related to each other.

II. A PRIMER ON CYBERSECURITY CONCEPTS

With the growth of cyberspace, the simultaneous growth of misuse of cyberspace has taken place. It's not only about how we use today's technology in our daily lives but also to be noticed that how well we are aware of what type of data we are using to communicate over the internet world. The concept of information security arises here, we can easily understand the importance of cybersecurity, similar to the daily used technology. Every individual has the right to their privacy, it is up to them what they want to share and with whom they want to share, but when private data becomes vulnerable and in any case gets into the hands of any evil individual it becomes a threat to that particular individual whose data has leaked, to protect any type of data that has to remain personal, private, and protected it should be maintained in such a way that it remains untouched by unauthorized communities or individuals. Below are some key concepts to know regarding cybersecurity.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205226 |

1. Threat Intelligence**:** Understanding current and emerging cyber threats is significant. This involves gathering, analyzing, and applying data about potential threats to enhance security posture. Gathering of data from various sources had been done using ontological methods, and there are various other models that was being used so as to achieve the goal of understanding the threats, which also had disadvantages attached to it[2].
2. Vulnerability Management**:** Vulnerability management is a cornerstone of cybersecurity, continuously identifying, assessing, and remediating vulnerabilities in systems and software to prevent exploitation by attackers.
3. Identity and Access Management (IAM)**:** Supervising and regulating user access permissions for systems and data to guarantee that only approved individuals can utilize designated resources.[3].
4. Encryption**:** Utilizing cryptographic techniques to secure data, both in transit and at rest, protecting it from unauthorized access. The effectiveness of their performance is influenced by multiple factors, including file size, format, intricacy, and the platform employed[4].
5. Network Security**:** Deploying firewalls, intrusion detection/prevention systems (IDS/IPS), and secure configurations to safeguard against network-based attacks.[5].
6. Endpoint Security**:** Ensuring the security of devices like computers, smartphones, and IoT devices by employing antivirus, anti-malware, and host intrusion prevention systems. Endpoint Detection and Response (EDR) tools are selected based on the understanding of Tactics, Techniques, and Procedures (TTPs).[6].
7. Security Awareness Training**:** Educating employees about cyber threats, best practices, and how to recognize and respond to suspicious activities[7].
8. Incident Response**:** Establishing procedures to detect, respond to, and recover from security incidents swiftly and effectively[8].
9. Security Testing**:** Performing routine evaluations like penetration testing and security audits to pinpoint vulnerabilities and authenticate security measures.
10. Regulatory Compliance**:** Adhering to industry-specific regulations (e.g., GDPR, HIPAA) and standards (e.g., ISO/IEC 27001) to ensure data protection and legal compliance.
11. Cybersecurity Frameworks**:** Following established frameworks like the NIST Cybersecurity Framework or CIS Controls to guide and organize cybersecurity efforts[8].
12. Cloud Security**:** Implementing security measures specific to cloud environments, including data encryption, access controls, and secure APIs.
13. Zero Trust Security**:**Embracing a model in which no entity is inherently trusted, necessitating verification for every user and device seeking access to resources.[9].
14. Machine Learning and AI**:** Utilizing advanced technologies to enhance threat detection, automate responses, and analyze vast amounts of security data for anomalies.
15. Secure Software Development**:** Incorporating security protocols across the software development lifecycle to detect and address vulnerabilities at an early stage.

III. VISUALIZATION OF AI IN CYBER SECURITY

Artificial Intelligence (AI) refers to the simulation and emulation of human intelligence processes through the development of computer systems and software. This broad domain encompasses an array of sophisticated technologies and methodologies geared towards empowering machines to execute tasks typically reliant on human intelligence, like learning, problem-solving, and decision-making. The potential of AI to transform numerous industries is vast, as it presents opportunities to automate operations, boost efficiency, and facilitate inventive solutions to intricate challenges. Given the broad definition of AI and its capabilities, it is easy to understand the significant value it holds for the field of information security. AI-powered systems can leverage a diverse array of algorithms and techniques to bolster security measures and achieve the overarching goal of safeguarding sensitive data and critical infrastructure. These techniques span a spectrum of applications, including classification, clustering, prediction, and in-depth data analysis. As the capabilities of AI continue to evolve, the integration of these technologies within information security frameworks promises to yield increasingly robust and adaptive security solutions.

a) Threat Intelligence**:** AI algorithms have the capability to analyze extensive volumes of data sourced from various outlets, detecting patterns, trends, and signs of compromise. This empowers organizations to anticipate and preemptively safeguard against emerging threats.

b) Vulnerability Management: AI-powered vulnerability scanners can automatically identify and prioritize vulnerabilities based on their severity, helping security teams focus on critical issues and remediate them promptly.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205226 |

c) Identity and Access Management (IAM): Authentication systems powered by AI can examine user behavior and contextual cues to identify anomalies and unauthorized access attempts. This fortifies access controls and diminishes the risk of identity theft.

d) Encryption: AI algorithms can enhance encryption techniques by optimizing key management, ensuring secure cryptographic protocols, and detecting potential weaknesses or vulnerabilities in encryption implementations.

e) Network Security: Intrusion detection and prevention systems (IDS/IPS) driven by AI can promptly detect and counter network-based attacks, employing machine learning algorithms to recognize abnormal traffic patterns and behavioral irregularities suggestive of potential threats in real-time[3].

f) Endpoint Security: AI-powered endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions can identify and counter advanced malware, ransomware, and zero-day attacks by analyzing real-time file behavior, process activity, and system events[6].

g) Security Awareness Training: AI-powered phishing detection and simulation tools can analyze email content, sender behavior, and user responses to identify and mitigate phishing attacks, while also providing personalized training and awareness programs based on user behavior.

h) Incident Response: AI-driven security orchestration, automation, and response (SOAR) platforms optimize incident response procedures by automating mundane tasks, coordinating workflows, and correlating security incidents from various origins to expedite incident detection, analysis, and resolution.

i) Security Testing: AI-driven penetration testing tools can simulate sophisticated cyber attacks, identify vulnerabilities, and provide actionable recommendations for improving security defenses, while also automating the testing process to scale and adapt to evolving threats.

j) Cloud Security: AI-powered cloud security solutions can monitor and analyze cloud infrastructure, detect misconfigurations, and enforce security policies to protect sensitive data and workloads in cloud environments, ensuring compliance with industry regulations and standards.

Machine-learning technology has detected 63,500 previously recognized threats across over 5,000 networks, encompassing zero-day exploits, insider threats, and covert, clandestine attacks[10].
It can be easily noticed that AI has automated tasks and bought drastic changes in the present technology but there are also several challenges that are been faced by it.
Here are few challenges that are to be faced by AI:

IV. CHALLENGES FACED BY AI

These are just some of the major challenges facing AI. As the field continues to evolve, researchers and developers are working on solutions to address these issues and pave the way for a more robust, ethical, and beneficial future of AI.

A. Data Issues:

a) Data Availability: Training effective AI models often requires massive amounts of data. Limited access to high-quality, labeled data can restrict the development and performance of AI systems. Researchers are exploring ways to leverage smaller datasets and generate synthetic data to address this challenge.

b) Data Bias: The effectiveness of AI models hinges on the quality of the data they're trained with. Biases within the data can result in discriminatory or unjust outcomes. Mitigating bias in data collection and algorithms is crucial to ensure AI systems are unbiased and equitable.

c) Data Privacy: The vast amount of data required for AI training often raises privacy concerns. Balancing the need for data with user privacy regulations is a complex challenge that requires innovative approaches to data management and protection.

By addressing these data-related challenges, the AI community can develop more reliable, trustworthy, and responsible AI systems that can truly benefit humanity.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205226 |

B. Technical Challenges:

a) Explainability and Transparency: A key challenge with many AI models is their inherent complexity, which can make them resemble black boxes. Understanding the reasoning behind the decisions these models make is often difficult, undermining trust in the technology and hindering efforts to debug and improve it. Addressing this issue of explainability is crucial for broader AI adoption and responsible development.

b) Limited Reasoning and Common Sense: While AI has demonstrated remarkable capabilities in specialized tasks, it often struggles with the general reasoning and common sense that comes naturally to humans. This limitation can prevent AI systems from adapting effectively to novel situations or understanding the broader context beyond the specific problem they were designed to solve. Bridging this gap in human-like reasoning is an ongoing area of research and development.

c) Computational Requirements: Training powerful AI models can be an extremely resource-intensive process, often requiring significant computing power and storage capacity. The high computational demands associated with advanced AI can translate to substantial financial costs, limiting the accessibility of this technology to smaller organizations and individuals. Developing more efficient AI algorithms and hardware solutions is crucial for making this transformative technology more widely available and affordable.

V. CONCLUSIONS

As reviewed in one of the papers [10], it can be noticed how cybersecurity may pose a danger for the future of cybersecurity. The paper included a speech by former US President Obama, where he discussed how powerful AI can not only increase automation for safety but also increase automation for attacks. That is man can use it for both good and bad, However, there is an easy solution: protecting the AI systems themselves. Before implementing the system, it becomes necessary to apply cybersecurity to AI first. Monitoring the work of AI is important for humans to ensure it does not lead to unintended actions. By securing the AI systems, we can harness their power for beneficial purposes while mitigating the risks of misuse or exploitation. Robust cybersecurity measures, such as encryption, access controls, and anomaly detection, must be put in place to safeguard the AI systems from potential threats. This proactive approach will not only enhance the reliability and trustworthiness of AI but also pave the way for its widespread adoption in critical domains. Ultimately, by prioritizing the cybersecurity of AI, we can unlock the full potential of these transformative technologies while ensuring the safety and security of our digital landscape. It has also to be noticed that AI which helps in cybersecurity must be a step ahead from cybersecurity helping in odds, though that may be a great race. Also the intelligence of computers must be under control of humans, so that it doesn't over take human behaviours. AI has been helping a lot and has taken all technology to great heights, but community should not forget about its artificial nature, and humans are responsible for its control, "As technology varies according to needs, same it can be manipulated as per human needs".

REFERENCES

[1] Yampolskiy, Roman V., and M. S. Spellchecker. "Artificial intelligence safety and cybersecurity: A timeline of AI failures." *arXiv preprint arXiv:1610.07997* (2016).

[2] Mavroeidis, Vasileios, and Siri Bromander. "Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence." *2017 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 2017.

[3] Devlekar, Sanket, and Vidyavati Ramteke. "Identity and Access Management: High-level Conceptual Framework." *REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS* 11.4 (2021): 4885-4897.

[4] Alenezi, Mohammed N., Haneen Alabdulrazzaq, and Nada Q. Mohammad. "Symmetric encryption algorithms: Review and evaluation study." *International Journal of Communication Networks and Information Security* 12.2 (2020): 256-272.

[5] Amarudin, R. Ferdiana and Widyawan, "A Systematic Literature Review of Intrusion Detection System for Network Security: Research Trends, Datasets and Methods," 2020 4th International Conference on Informatics and Computational Sciences (ICICoS), Semarang, Indonesia, 2020, pp. 1-6, doi: 10.1109/ICICoS51170.2020.9299068. keywords: {Support vector machines;Machine learning algorithms;Systematics;Bibliographies;Intrusion detection;Market research;Classification algorithms;Intrusion Detection System (IDS);Network Securty;Dataset;Machine Learning;Systematic Literature Review (SLR)},

[6] W. U. Hassan, A. Bates and D. Marino, "Tactical Provenance Analysis for Endpoint Detection and Response Systems," 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 1172-1189, doi:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205226 |

10.1109/SP40000.2020.00096. keywords: {Tools;Security;Skeleton;Knowledge based systems;Fatigue;Task analysis;Manuals},

[7] Dash, Bibhu, and Meraj F. Ansari. "An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy." (2022).

[8] Staves, Alexander, et al. "A Framework to Support ICS Cyber Incident Response and Recovery." *ISCRAM*. 2020.

[9] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," in IEEE Access, vol. 10, pp. 57143-57179, 2022, doi: 10.1109/ACCESS.2022.3174679.keywords: {Access control;Authentication;Computer architecture;NIST;Encryption;Critical infrastructure;Automation;Zero trust architecture (ZTA);access control;authentication;micro-segmentation;software-defined parameter (SDP)},

[10] Goosen, Ryan, et al. "ARTIFICIAL INTELLIGENCE IS A THREAT TO CYBERSECURITY. IT'S ALSO A SOLUTION." *Boston Consulting Group (BCG), Tech. Rep* (2018).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details