International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 8, No. 2, 2021, pp. 11-15.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Improving Cybersecurity Using Artificial Intelligence: Overview, Modeling, Future Directions

Ananya Mehra [a], Rohit Iyer [b]

[a] *Centre for AI Ethics, Pune Institute of Cognitive Sciences, India.*
[b] *Centre for AI Ethics, Pune Institute of Cognitive Sciences, India.*

Abstract

This article examined the application of Artificial Intelligence (AI) in mitigating cybersecurity challenges. While safe communication among individuals, services, and gadgets is achievable through centralized digital entities, considerable risks accompany digital transformation. Data mining, targeting, and exploitation can occur without users' consent. The ongoing delivery of centralized solutions by service providers is inefficient due to redundancy, possesses considerable security vulnerabilities, and presents consumer challenges. Verification and validation of digital identifiers are essential for safeguarding the privacy and safety of decentralized online identities. The current body of knowledge lacks comprehensive studies regarding unified communication components and the security and confidentiality of user information protocols used in systems that manage identities. Digital authentication and validation are undoubtedly among the most possible uses of the technology known as blockchain. Distinct security breaches impacted billions of persons globally. Better secure techniques for storing, transmitting, and verifying private information are necessary. In this regard, advancing blockchain technology for identity systems provides effective remedies for specific challenges centralized databases encounter. Equipment and human intervention are insufficient to mitigate and safeguard against hacking. The criminals exploit the Internet to commit various cybercrimes. The specialists require support in averting attacks and security violations, as well as in addressing attacks. The principal aim of security is to mitigate attacks by applying AI techniques. AI is currently applied in information security, and AI methodologies can mitigate specific cybersecurity challenges alongside many advantageous AI uses.

Keywords: Cybersecurity, Artificial Intelligence.

Received: 06 March 2021/Revised: 09 April 2021/Accepted: 5 May 2021/Published: 30 June 2021

Introduction

Synopsis of the Cybersecurity (CS) Environment

Security has become a paramount concern for people, enterprises, and authorities in the interconnected digital landscape (Sulich et al., 2021). The exponential increase in web surfing and the growing number of electronic gadgets have significantly enlarged the attack field for online dangers. The field of CS is ever-evolving, presenting formidable challenges due to breaches of information, attacks involving ransomware, and advanced hacking campaigns aimed at critical systems. As technology progresses, the strategies and methods utilized by cybercriminals evolve, necessitating enterprises to remain aware and proactive in safeguarding against changing risks.

Expanding Significance of Artificial Intelligence (AI) in Security

The emergence of Artificial Intelligence as a powerful instrument in supplementing CS measures is seen in today's volatile environment of threat (Li, 2018). By employing AI systems, extensive datasets can be analyzed, patterns can be identified, and abnormalities can be identified at rates and scales much beyond those available to humans. Then, AI bases cybersecurity in which real-time threats can be detected and addressed through real-time machine learning techniques and statistical analysis to keep businesses ahead of hackers. With the growth in volume and complexity of cyber threats, AI has become an integral part of cybersecurity, ultimately changing the means of threat identification, avoidance, and incident handling.

Statement of the Problem

Although AI can potentially reinforce CS measures promptly, much needs to be solved regarding challenges and unknowns (Nishant et al., 2020); traditional approaches to CS often cannot keep up with the fast evolution of cyber threats, thus leaving defenses weak and vulnerable to exploitation by attackers. With the AI-enabled solution comes the question of privacy, ethics, and unforeseen consequences, posing significant questions in finding the right balance between security and individual freedom. It is imperative first to understand the benefits and limitations of AI inefficient, real-life CS scenarios and then figure out the best way of integrating AI into existing CS systems (Sobb et al., 2020).

Background

The historical perspective of computer security risk is crucial in understanding the evolution of electronic security threats and the continuous need to improve security mechanisms. The past few decades have witnessed a remarkable evolution of computer security threats, often synchronized with the pace of technological breakthroughs. During the initial stages of computer evolution, computer security issues were directly related to keeping the access of unwanted people outside the mainframe networks and systems. At this point, the threats were simple and often appeared as infections or thread attacks. These viruses and threads traveled frequently through physical mediums like floppy disks and thus posed a considerable danger to early computers (Perwej et al., 2021).

The extensive proliferation of the Internet has radically turned into a paradigm of cyber assaults that use pathways in internal interconnected systems to propagate further and cause damage. A new paradigm of cyber threats has begun, characterized by the initiation of increasingly sophisticated attack techniques. Malware, from which the most widely conventional forms are trojans and ransomware, is widely available for generally causing havoc upon networks. Denial-of-Service (DoS) attacks were developed to minimize an internet resource's availability by flooding target servers with excessive malicious traffic (Huseinović et al., 2020). It now generalizes to breach of data, which involves illegal access and leakage of private data from both organizations and individuals. Enterprises face multifarious CS threats and challenges in the contemporary connected and digital world. Attack forms by hackers have increased in types and complexities and are targeted at large companies, small enterprises, and even individuals (Bendovschi, 2015). Attack types have continued to evolve, including the theft of vital data through encryption and ransom payments to decrypt such data. Those have been on the rise in the past years, resulting in lost funds and operations interruptions. They pose a significant concern because phishing attacks's methodology involves using deceptively fraudulent emails or webpages by hackers to lure victims into divulging critical information. The malicious acts perpetrated by rogue or unaware insiders further prevent CS defenses in organizations from being effective. The growing usage of IoT gadgets and cloud computing has also presented new attack vectors while stretching CS management to greater complexity (Srivastava et al., 2020).

With the change towards AI came new perspectives on what CS could achieve in rehabilitating threat detection, prevention, and response capabilities. Earlier AI in CS would mostly be pattern rule derived, using signatures or patterns defined in advance to detect known threats. As cyber threats evolved in sophistication and dynamism,

conventional signature-based techniques were impotent to detect zero-day assaults and polymorphic software. This created a demand for the birth of AI-driven safety measures that use Machine Learning (ML) techniques to scrutinize giant sets of bits to detect anomalies in behavior, suggesting possible dangers. AI is transitioning into predicting cyber risks using post-variance data and has an advantage over most network defenders using network formation.

Challenges and Limitations

AI promises to provide better protections and prophylactic measures against threats that are developing quickly in the rapidly dynamic field of CS. However, several obstacles and limitations must be taken into consideration by this technical miracle. It is also not easy to assess the technical capabilities of AI systems while probing into CS ethical, human, and regulatory aspects.

Ethical Implications of AI in CS

With the advent of sophisticated AI algorithms, ethical dilemmas are beginning to raise considerable dust in the CS landscape. Incorporating AI into CS provokes questions about essential privacy, autonomy, and responsibility. On the other hand, much of the data procured by AI-driven systems are from large datasets; hence, data privacy and possible mischief come into play. Next, the inscrutable nature of the ML algorithms confuses the decision-making processes under which they relate to matters of responsibility and transparency. The ethical considerations, as shown by that tussle between security and personal liberties, require a holistic ethical framework that will direct the development and deployment of AI in CS.

Technical Obstacles and Constraints of AI-Driven Defenses

Notwithstanding the richest promise that AI may breathe into CS, technical challenges or restrictions exist. One of the significant challenges involves sabotage against, or hacking of, the AI system. Cyber attackers might exploit weaknesses in AI algorithms or misuse methods like adversarial instances to mislead AI-driven defenses into making erroneous conclusions. Artificial intelligence systems are supposed to be capable of quick and instantaneous changes and adaptations as the nature of cyber threats changes. However, getting that speed with precision and reliability is a significant technical challenge. Furthermore, reliance on AI presents additional failure measures since attackers exploit system problems or limitations in algorithms used by AI.

In CS solutions offered by AI, human behavior is considered a significant element in the effectiveness of the defense mechanism. AI systems provide humans with outcome treatment and decision-making responsibility, which have serious consequences. Human-machine interaction defies simplistic models. Misunderstanding of AI-generated alerts or over-reliance on AI systems could produce false positives or negatives in either case, rendering CS mechanisms replicable effectively. CS professionals' lack of understanding of AI technology is a major stumbling block to the full exploitation of AI-powered solutions altogether.

Legislative and Compliance Issues

Artificial intelligence in cybersecurity has other rules and compliance challenges. New legal ways for AI technologies are still awaited, with just a few general regulations created explicitly for cybersecurity applications. Every extra complicated particularity required by the compliance obligations, such as data protection laws and industry norms, adds more complexity to using AI-enabled protection.

Cross-border data flows, and international collaboration in CS initiatives raise jurisdictional and nationality issues. Handling the regulatory and compliance hurdles is essential to ensure that AI-based CS solutions are consistent with legal and ethical standards without compromising efficiency in safeguarding digital assets. With the implementation and dealing with complicated problems and limitations tied to this, AI may impart huge potential improvements to CS measures. Ethical, technical, human, and legal issues must be considered carefully while maximizing the functions of AI in securing our digital infrastructures. The research can ensure the responsible and practical use of AI for safety through proper understanding and proactive addressing of these challenges.

Future Directions and Recommendations

Prospective Enhancements in AI for CS

Advancements in technology have created a possibility for AI in security that is promising and relevant to preventing cyber threats. AI systems can be made with greater capacities to identify and predict cyber threats. These approaches include using sophisticated machine learning techniques (such as Deep Learning) to quickly examine vast volumes of data for subtle patterns indicative of an attack. The merging of AI with other emerging technologies, such as

Blockchain and Quantum Computing, shows excellent prospects for augmenting countermeasures for computer security. AI-based Blockchain systems enhance information security and integrity, while Quantum Machine Learning algorithms could strengthen encryption schemes against quantum computer threats. Research into explaining AI (XAI) augments transparency and trust in AI security systems. XAI generates an understanding of the AI algorithm's decision-making processes, giving CS practitioners confidence in understanding and interpreting the system's outputs, thereby allowing for better defense and mitigation strategies.

Strategies for Integrating AI into Established CS Frameworks

Integrating AI into established security systems is a deliberate exercise that entails a systematic approach to ensure a smooth passage and, hence, the maximum effectiveness of the algorithms. It is recommended that limited AI implementations in areas like threat identification or incident handling be the starting point for broader implementations of AI in CS.

Collaboration between AI producers, CS suppliers, and other groups should happen so that AI products that adequately address the discrete security demands of different businesses and sectors can be developed. Investment in education and training for CS personnel so that they can maximize the use of AI tools should be made by these entities. This could include training on AI methodologies and tactics and fostering a culture of continuous learning and flexibility to meet the advancing cyber threats.

Suggestions for Politicians, Companies, and Security Experts

The policy Shi-er has an essential position in formulating the regulatory framework for AI and CS. Establish default standards and norms about ethical practicalities in using AI in CS that safeguard against bias and prejudice in AI systems. Organizations should now label CS as a strategic need and, with proper allocation and resourcing, invest in AI-driven safety measures. They will create a working environment of collaboration and knowledge sharing internally and externally to augment collective cyber resilience. CS practitioners would be constantly updated about new developments in AI and consistently update their skills and capabilities to bring about judicious application of AI technology within their roles. They should stay on top of all the latest emergent threats and adjust their security measures proactively to stay ahead of attackers.

Regions for Further Studies

However, even though they have already entailed substantial progress toward AI for information security, there remains a spectrum that requires additional investigations to tackle mostly prevalent obstacles and reveal newer opportunities:

- Scaling up and providing efficiency to AI systems concerning real-time identification and response to threats.
- The capacity of AI-driven solely independent CS systems to improvise and adapt owing to dynamic online threats.
- Application of AI to malware recognition and gathering information regarding APTs, intending to discover and counteract it.
- Identifying ethical and privacy notions of AI in CS, which includes issues such as protecting information and transparency on algorithms.
- Examining the human aspects relevant to AI-driven CS structures like customer trust and adoption of AI recommendations.
- By concentrating on these study domains, the study further advances the field of AI-driven security and establishes more robust defenses versus upcoming digital hazards.

Conclusion

This study analyzes the role of AI in mitigating CS challenges. This research indicates that AI is rapidly becoming an essential instrument for enhancing the efficacy of information security organizations. People can no longer effectively secure an enterprise-level attack. AI offers critical analysis and detection of threats that security experts can leverage to diminish the likelihood of a breach and enhance their organization's security posture. As information becomes increasingly integrated into our daily existence, AI's impact on our lives will escalate. Some experts contend that AI would adversely affect technology, but others assert that AI will substantially enhance human lives. The principal benefit of using cloud computing in security is the capacity to evaluate and neutralize threats with incredible speed.

The ability of hackers to execute progressively advanced cyber and technology-driven attacks is a significant concern for many individuals. Moreover, AI can facilitate the recognition and ranking of risks, guide responses to incidents, and detect malware attacks before occurrence. Despite potential limitations, AI will enhance CS and enable enterprises to establish a more robust security stance.

References

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia Computer Science*, *192*, 20-28. https://doi.org/10.1016/j.procs.2021.08.003.

Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474. https://doi.org/10.1631/FITEE.1800573.

Nishant, R., Kennedy, M., & Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. *International journal of information management*, *53*, 102104. https://doi.org/10.1016/j.ijinfomgt.2020.102104.

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11), 1864. https://doi.org/10.3390/electronics9111864.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04.

Huseinović, A., Mrdović, S., Bicakci, K., & Uludag, S. (2020). A survey of denial-of-service attacks and solutions in the smart grid. *IEEE Access*, *8*, 177447-177470. https://doi.org/10.1109/ACCESS.2020.3026923.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24-31. https://doi.org/10.1016/S2212-5671(15)01077-1.

Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P., & Aski, V. J. (2020). Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. *International Journal of Communication Systems*, *33*(12), e4443. https://doi.org/10.1002/dac.4443.