Library Progress International
Vol.44 No.3, Jul-Dec 2024: P.3253-3259

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Security against Cyber Threats Using Artificial Intelligence

Iratus Glenn A. Cruz

Program Coordinator and MIS Coordinator, College of Communication and Information Technology President Ramon Magsaysay State University, Philippines, igcruz@prmsu.edu.ph

How to cite this article: Iratus Glenn A. Cruz (2024). Security against Cyber Threats Using Artificial Intelligence. *Library Progress International*, 44(3), 3253-3259.

Abstract

In the virtual world, cybersecurity is essential for safeguarding data integrity and information systems. This paper investigates how cyber threats have evolved over time. From simple hacking efforts to sophisticated organised criminality, cyber threats have an impact on world economies. Numerous cyberattacks, including malware, phishing, and botnet attacks, take advantage of weaknesses and loopholes in digital systems to cause serious security concerns and loss for both persons and businesses. By facilitating better anomaly detection, real-time monitoring, and early threat identification, how the integration of artificial intelligence (AI) capabilities improves cybersecurity can be observed in this review.

Keywords-: Cyber security, Cyber threats, AI tools, AI detection, Threat prevention

Introduction

The term "cyber" refers to networks with infrastructure information systems, often known as "virtual reality". Cybersecurity is the protection of information systems generated by organisations, companies, and individuals in an electronic environment which involves data, communication, life, integration, and assets that are both tangible and intangible. In summary, cyber security guards virtual life on cyber networks. Cybersecurity is the protection of information systems infrastructure, confidentiality, and data integrity. Cybersecurity aims to protect individual and organisational data on the Internet. Ignorance of this vital knowledge can cause great risk to internet security.[1]. These threats are known as “cyber threats”.

A cyber threat is any intentional attempt to compromise, interfere with, or obtain unapproved access to computer networks, systems, or data. These threats may originate from people, organisations, or nation-states, and they may be motivated by various ideas, including espionage, financial gain, political action, revenge or personal motives, exploring new challenges and skills, or just making trouble. Cyber dangers come in numerous forms and can take advantage of the loopholes in systems, procedures, and human nature. [2]

A single security breach might compromise millions of people's personal information. This results in loss in customer’s confidence, and severe financial suffering to the organizations. Therefore, for providing shield to people and companies from spammers and other hackers, role of cyber security is must.[3]

It has been observed that integrating artificial intelligence (AI) into cybersecurity improves the detection of threats, response capabilities, and cybersecurity measures as a whole. AI makes early threat detection possible by using real-time monitoring and advanced threat detection techniques to scan data for odd patterns and behaviours.[4]

2. Unveiling the Evolution of Cyber Threats

Cybercrime emerged several years ago. The hacking attempts were not as sophisticated as they are now since there were less systems in the digital realm. At the time, defending the digital world was easier.

However as technology progressed over time, hackers began to use automated tools to execute out complex cyberattacks. Additionally, a wide range of devices and platforms, such as social media platforms, cloud platforms, IoT devices,

smartphones, and tablets, have been proposed to the Internet.[5]. Due to these reasons, cybercrime has evolved from humorous gags to highly strategic attacks that annually cost the global economy trillions of dollars in the digital sphere.

Table 1: Categories of cybercrimes over the years. [6]

Period	Description of Cyber Threats
1940s	Years with zero crime in computer field
1950s	Decade of Telephone hacking
1960s	Vulnerability terms & Hacking emerged
1970s	Computer security was established
1980s	Era of Advanced Research Projects Agency Network (A.R.P.A.N.E.T) to Internet
1990s	Popularity of Computer viruses
2000s	Excessive growth of Internet
2010s	Discovery of various breaches in computer systems related to security
2020s	Cyber crimeevolving as an industry

Table 1 displays how cybercrimes have evolved over the course of time, beginning in the 1940s when there were barely any crimes involving computers and continuing in the 2020s when cybercrime had developed into a major worldwide business that posed serious security and financial challenges. [6]

3. Types of Cyber Attacks

With the advancement of technology, the way in which information may be accessed has expanded. Due to ease in access to information, maintaining information security has become more difficult. With current computer technology immersed in many facets of society, the concept of cyberattacks has grown in significance. Cyberattacks have targeted government agencies, banks, hospitals, businesses, daily life, and the economy. [7]

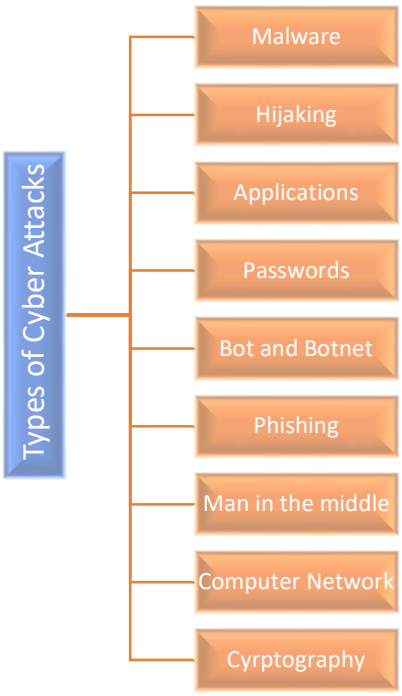

Fig 1- Common types of Cyber Attacks [8-11]

Figure 1 demonstrates some common types of cyber attacks in practice. These are Malware attacks, Hijacking, man-in-the-middle, Phishing, attacks via applications, bots & botnets, computer network attacks etc. Cyberattacks aiming to exploit distinct weaknesses in digital systems can take many different forms. [8-11]

Cyber threats such as hijacking includes gaining unauthorised access and damage to a computer, device, or session. Malware, on the other hand, is malicious software. Application attacks employ software flaws to get illegal access or do damage. [12] Password attacks try to break into or steal user credentials. Phishing includes posing as a reliable source by misleading attempts to steal sensitive information. [13]Attacks using bots and botnets harness invaded computer networks under remote control to carry out damaging activities. Computer network attacks target the infrastructure to interrupt services or steal data, while man-in-the-middle attacks intercept and modify communications between two parties.[14] Cryptography attacks concentrate on cracking encryption or taking advantage of flaws in the system. [15]

4. Use of AI tools to prevent Cyber fraud

Artificial intelligence (AI) is a vast field that uses variety of tools and technologies, such as machine learning, NLP, and other approaches, to improve threat detection, incident response, and overall security posture. AI tools together improve the capacity to identify, prevent, and respond to cyber fraud, resulting in stronger security measures in the digital realm.[16]. Figure 2 shows various AI tools and their brief description of usage in cyber security.

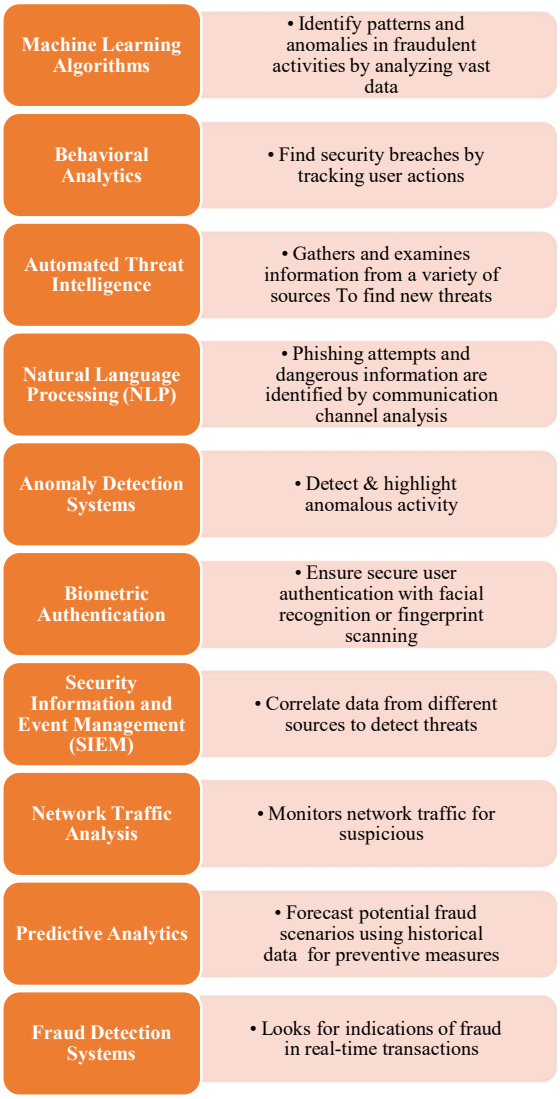

Fig 2-AI tools and their function in Cyber security [17-24]

Figure 2 illustrates AI tools and applications in cybersecurity. Machine Learning systems analyse massive amounts of data to detect trends and anomalies in fraudulent actions. Behavioural analytics track user behaviour to detect security vulnerabilities. AI-powered anomaly detection systems alert to unexpected behaviour, whereas fraud detection systems continually check for evidence of fraud in real-time transactions. Natural Language Processing (NLP) scans communication channels for phishing attempts and dangerous information. Automated Threat Intelligence gathers and analyses data from a variety of sources to detect new dangers. Artificial intelligence systems are used for biometric authentication. Predictive analytics predicts fraud scenarios and provides prevention actions. Suspicious activity is monitored by network traffic analysis. Security Information and Event Management combines AI to provide full threat detection and response capabilities in cyber security.[17-24]

5. Impact on Cyber security by integration of AI

Conventional cybersecurity technologies had drawbacks including poor scalability, high false positive rates, and delayed reaction times until AI was implemented. The frequency of cyberattacks and the expanding threat landscape put further strain on established defence systems.

With the integration of AI, there are several advantages. AI-powered systems are able to analyze enormous volume of data in real time and spot abnormal patterns more precisely than conventional approaches, leading to improved accuracy in threat detection and response. [25]. By learning from past data and making adjustments, machine learning algorithms

can lower false positives, giving security teams more targeted warnings and fewer false positives overall. Real-time response to crises by automated AI systems can mitigate hazards faster and lessen the effect of assaults.

The capacity of AI to recognise and react to unforeseen threats improves security posture overall. Subtle signs of compromise, such as odd user behaviour or patterns in network traffic, might be found via behavioural analysis. [26] Based on past data and trends, AI can also forecast possible dangers, giving organisations the ability to put proactive defences in place and reduce risks before assaults happen.

Because AI systems can learn and adapt over time, they can also be continually improved, making it easier for them to respond to changing cyber threats and attack methods.

Artificial intelligence-powered cyber security systems can detect and respond to threats more quickly by sifting through enormous volumes of data to find anomalous behaviour and hostile activities. [27]. They can simplify the task of staying on top of cyber security requirements by automating security procedures like patch management. Because AI-based systems can scan device for possible vulnerabilities in a fraction of time as compared with human operations, they also provide enhanced accuracy and efficiency over traditional solutions. Artificial intelligent systems are designed to identify patterns that a human eye might find difficult to see, improving the accuracy of detection of harmful activites. [28]

Because AI based solutions automate time-consuming security processes and handle large volumes of data properly and fast, they also provide increased scalability and cost savings. [29]

6. Conclusion

The paper gives a brief knowledge of cyber threats and the need for security in the digital ecosystem. The motive behind these frauds is put on along with the loss created by cyber crimes worldwide. Evolution from the 1940s to the present date has been described. The review covers various trending types of cyber attacks and how they exploit the security of data has been discussed. Study shows that the integration of artificial intelligence (AI) in cybersecurity turns out to be a significant step forward in protecting digital ecosystems. With emerging cyber crimes as an industry over time, AI-powered tools and systems are used to manage threats with their vast and quick abilities. AI has been used in cyber security for

- identifying and responding to abnormalities in real-time
- Strengthening defences against sophisticated cyber threats.
- Monitoring network traffic
- Securing authentication
- Tracking user action and abnormalities in pattern
- Forecasting fraud scenarios
- improving threat detection accuracy and efficiency

AI tools such as machine learning (ML) and predictive analytics, also helps in mitigating false positives. Furthermore, AI's adaptable nature allows for continual refinement of response techniques, providing organisations with proactive defences against evolving cyber threats. As the digital ecosystem changes, AI is critical in strengthening cybersecurity frameworks and maintaining resilience to the dynamic threats offered by hackers. In the last segment of the paper, transformation in cyber security before and after the integration of AI is discussed. It can be concluded that AI can significantly enhance cybersecurity operations in a variety of ways. Large data sets may be intelligently examined by AI-powered systems, allowing for the discovery of patterns and anomalies which have been previously hidden. This diminishes the potential effect of any harm by enabling proactive threat identification and response towards risk in cyber security.

References

[1] Aslan, Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." *Electronics* 12, no. 6 (2023): 1333.

[2] Ghelani, Diptiben. "Cyber security, cyber threats, implications and future perspectives: A Review." *Authorea Preprints* (2022).

[3] Perwej, Yusuf, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, and Anurag Kumar Jaiswal. "A systematic literature review on the cyber security." *International Journal of scientific research and management* 9, no. 12 (2021): 669-710.

[4] Kaur, Ramanpreet, Dušan Gabrijelčič, and Tomaž Klobučar. "Artificial intelligence for cybersecurity: Literature review and future research directions." *Information Fusion* (2023): 101804.

[5] Tang, Yi, Qian Chen, Mengya Li, Qi Wang, Ming Ni, and XiangYun Fu. "Challenge and evolution of cyber attacks in cyber physical power system." In *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, pp. 857-862. IEEE, 2016.

[6] Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. "Measuring the changing cost of cybercrime." In *The 18th Annual Workshop on the Economics of Information Security (WEIS 2019)*. 2019.

[7] Gunduz, M. Zekeriya, and Resul Das. "Analysis of cyber-attacks on smart grid applications." In *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, pp. 1-5. IEEE, 2018.

[8] Duo, Wenli, MengChu Zhou, and Abdullah Abusorrah. "A survey of cyber attacks on cyber physical systems: Recent advances and challenges." *IEEE/CAA Journal of Automatica Sinica* 9, no. 5 (2022): 784-800.

[9] Al-Mohannadi, Hamad, Qublai Mirza, Anitta Namanya, Irfan Awan, Andrea Cullen, and Jules Disso. "Cyber-attack modeling analysis techniques: An overview." In *2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW)*, pp. 69-76. IEEE, 2016.

[10] Inayat, Usman, Muhammad Fahad Zia, Sajid Mahmood, Haris M. Khalid, and Mohamed Benbouzid. "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects." *Electronics* 11, no. 9 (2022): 1502.

[11] Al-Khater, Wadha Abdullah, Somaya Al-Maadeed, Abdulghani Ali Ahmed, Ali Safaa Sadiq, and Muhammad Khurram Khan. "Comprehensive review of cybercrime detection techniques." *IEEE access* 8 (2020): 137293-137311.

[12] Ali, Mazurina Mohd, and Nur Farhana Mohd Zaharon. "Phishing—A Cyber Fraud: The Types, Implications and Governance." *International Journal of Educational Reform* 33, no. 1 (2024): 101-121.

[13] Datta, Priyanka, Surya Narayan Panda, Sarvesh Tanwar, and Rajesh Kumar Kaushal. "A technical review report on cyber crimes in India." In *2020 International conference on emerging smart computing and informatics (ESCI)*, pp. 269-275. IEEE, 2020.

[14] Hidayati, Anisa Nur, Imam Riadi, Erika Ramadhani, and Sarah Ulfah Al Amany. "Development of conceptual framework for cyber fraud investigation." *Register* 7, no. 2 (2021): 125-135.

[15] Fernandez-Carames, Tiago M., and Paula Fraga-Lamas. "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks." *IEEE access* 8 (2020): 21091-21116.

[16] Hassan, Moahammad, Layla Abdel-Rahman Aziz, and Yuli Andriansyah. "The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance." *Reviews of Contemporary Business Analytics* 6, no. 1 (2023): 110-132.

[17] Ansari, Meraj Farheen, Pawan Kumar Sharma, and Bibhu Dash. "Prevention of phishing attacks using AI-based Cybersecurity Awareness Training." *Prevention* 3, no. 6 (2022).

[18] Xu, Jinxin, Han Wang, Yuqiang Zhong, Lichen Qin, and Qishuo Cheng. "Predict and Optimize Financial Services Risk Using AI-driven Technology." *Academic Journal of Science and Technology* 10, no. 1 (2024): 299-304.

[19] Ashfaq, Tehreem, Rabiya Khalid, Adamu Sani Yahaya, Sheraz Aslam, Ahmad Taher Azar, Safa Alsafari, and Ibrahim A. Hameed. "A machine learning and blockchain based efficient fraud detection mechanism." *Sensors* 22, no. 19 (2022): 7162.

[20] Capuano, Nicola, Giuseppe Fenza, Vincenzo Loia, and Claudio Stanzione. "Explainable artificial intelligence in cybersecurity: A survey." *IEEE Access* 10 (2022): 93575-93600.

[21] Yeboah-Ofori, Abel, Shareeful Islam, Sin Wee Lee, Zia Ush Shamszaman, Khan Muhammad, Meteb Altaf, and Mabrook S. Al-Rakhami. "Cyber threat predictive analytics for improving cyber supply chain security." *IEEE Access* 9 (2021): 94318-94337.

[22] Obaidat, Mohammad S., Issa Traore, and Isaac Woungang, eds. *Biometric-based physical and cybersecurity systems*. Cham: Springer International Publishing, 2019.

[23] Ukwen, David Okore, and Murat Karabatak. "Review of NLP-based systems in digital forensics and cybersecurity." In *2021 9th International symposium on digital forensics and security (ISDFS)*, pp. 1-9. IEEE, 2021.

[24] Diaz Lopez, Daniel, María Blanco Uribe, Claudia Santiago Cely, Andrés Vega Torres, Nicolás Moreno Guataquira, Stefany Morón Castro, Pantaleone Nespoli, and Félix Gómez Mármol. "Shielding IoT against cyber-attacks: an event-based approach using SIEM." *Wireless Communications and Mobile Computing* 2018, no. 1 (2018): 3029638.

[25] Sontan, Adewale Daniel, and Segun Victor Samuel. "The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities." *World Journal of Advanced Research and Reviews* 21, no. 2 (2024): 1720-1736.

[26] Manoharan, Ashok, and Mithun Sarker. "Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection." *DOI: https://www. doi. org/10.56726/IRJMETS32644* 1 (2023).

[27] Johnson, James. "Artificial intelligence & future warfare: implications for international security." *Defense & Security Analysis* 35, no. 2 (2019): 147-169.

[28] Zeadally, Sherali, Erwin Adi, Zubair Baig, and Imran A. Khan. "Harnessing artificial intelligence capabilities to improve cybersecurity." *Ieee Access* 8 (2020): 23817-23837.

[29] Nadella, Geeta Sandeep, and Hari Gonaygunta. "Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT." *International Journal of Science and Engineering Applications* 13, no. 04 (2024): 30-33.