World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

A comprehensive review of cybersecurity challenges in the post-pandemic world: The role of AI in mitigating threats

Adeyemi Afolayan Adesola [1,*] and Awele Mary-rose Ilusanmi [2]

[1] *Department of Computer Science; Stephen F. Austin State University; Nacogdoches; Texas; USA.*
[2] *Department of Multidisciplinary Studies, College and Liberal Arts; Stephen F. Austin State University; Nacogdoches; Texas; USA.*

World Journal of Advanced Research and Reviews; 2025, 25(02), 1005-1011

Publication history: Received on 27 December 2024; revised on 02 February 2025; accepted on 05 February 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.2.0402

Abstract

COVID-19 not only impacted the overall digital environment but also forced companies around the world to adapt rapidly to new working models, cloud service, and digital transformation. The changes which allowed business to go on also brought in new threats related to cybersecurity. To defend against these new threats and improve threat identification, event management, and organizational security, this paper will look at the several ways artificial intelligence (AI) is being incorporated into cybersecurity solutions. Artificial Intelligence introducing intelligent algorithms that analyze patterns and detect threat patterns in real time. The study shows how AI can adapt dynamically to existing risks, perform effective optimization of repetitive tasks, analyze polymorphic viruses and help in minimizing burden on a cybersecurity team and improve the chances of executing a reliable strategy for increased solutions to issues and challenges. Moreso, the study also highlights the issue of data quality management, the adherence to ethical practices and research cooperation to optimize the potential of the techniques.

Keywords: Artificial Intelligence; Polymorphic virus; Threat detection; Cloud Security

1. Introduction

COVID-19 influenced the global digital environment drastically changing the dynamics of the entire world and offering situations that no one had encountered before. The internet is relied upon as the tool for working, learning, connecting and even buying and selling as the world went into locking down and practicing physical social distance. However, this structurally driven and digital based approach revealed significant flaws in businesses [1]. Businesses that were not ready for any form of such a shift realized that the cybersecurity threats they face has increased because the cyber-criminals were taking advantage of situations like this. Among the most worrying deficiencies, there were virtually no effective measures in place for guarding against threats posed by cyber threats facing remote workforce [2-3]. The workers relocated to remote working, which has been on both personal devices and insecure networks. This change extended corporate networks, by allowing connection to internal networks thereby exposing them to the dangers of cyber threats. But regrettably, attackers could not overlook these flaws and went on to launch deliberate phishing and contemporary attacks using ransomware that allowed them to get access to several systems and steal important data outright [4].

The kind of threats also changed during and after the pandemic and these are nation-state actors, and other different types of cybercriminal groups, started incorporating the new technologies like Artificial Intelligence (AI), and Machine Learning (ML), to boost the efficiency and success of the attacks, taking it to the next level. Specifically, the level of sophistication with which malicious actors designed their messages and approached their intended targets increased,

* Corresponding author: Adeyemi Afolayan Adesola ORCID: 0009-0004-4325-5641

malware became much more capable of avoiding detection by anti-virus software, and ransomware attacks became more assertive in their methods. That is why today organizations have much more diverse and complex threat environment to deal with [5].

Critical infrastructure, health care delivery systems, and supply lines have all been attacked to show that disruption is possible. Indeed, in an increasingly connected world, cybersecurity has moved from being the responsibility of organizations, institutions and businesses, but rather something that affects the world, and therefore requires intervention from all members of society and especially scientists [4]. The COVID-19 outbreak was followed by a growing number of cyberattacks as attackers acted on fear and disruption caused by the pandemic [6]. Hackers developed sophisticated scams, spread fake news, and fake relief with the aim of stealing data and exploiting unsuspecting employees. Several organizations including governments agencies suffered from series of attacks ranging from stealing data to service disruption. Due to the abrupt nature of the COVID-19, many of the attacks during the pandemic were successful as many organizations have little time to prepare for the sudden transition to remote work, loss of key employees, use of outdated security measures, as well as being under-equipped to counter these threats [7-9].

The pandemic led to new changes in people's working conditions, and one of the most significant changes was remote work. While this helped businesses to continue their operation it has also caused a lot of cybersecurity issues. Some employees started working from home and did not know how to secure themselves from cyber threats . Most employees were connecting to secure internal networks through unsecure Wi-Fi and personal devices that lack strong encryption. These weaknesses were seized by cybercriminals who launched different attacks within a short time. For instance, attackers used a brute force attack approach to gain access to weak remote access systems. Phishing schemes targeting remote workers became more prevalent as hackers try to obtain login credentials so they may access confidential information. Today, companies realize the importance of deploying secure tools, raising and educating employees, creating the correct cybersecurity policies to work safely and efficiently in new hybrid environments [10-11].

Businesses were under massive pressure to adapt to the digital environment as soon as the pandemic emerged. The fast pace of adopting new information technologies was crucial for business continuity. However, it was accompanied by significant risks to companies' information security. Numerous companies began utilizing cloud services, teamwork tools, and e-commerce platforms without understanding the security risks or without sufficient safeguards.

2. Challenges in Cloud Security

There has been a massive increase in the adoption of cloud services due to the pandemic as business requires flexible solutions to accommodate remote employees and online operations. Such swift changes brought new concerns with it. Some of the concerns include wrong configurations on cloud platforms, lack of adequate security measures and weak encryptions resulting in threat actors intercepting data in transit [12]. Ransomware attacks have increased significantly since the covid 19 pandemic impacting several organizations by encrypting vital data and requiring a ransom to allow access to the encrypted data. A major contributor to this is the availability of Ransomware as a Service (RaaS) model which helps even inexperienced attackers pull off highly technical attacks. These platforms present tools, support and infrastructure for even script kiddies to turn a profit from ransomware attacks. Victims of ransomware face tough choices, they either pay the ransom and open to more attacks or experience disruption of critical infrastructures [8, 13-14].

Despite cybersecurity being heavily rooted in technology, humans remain a major weakness. Social engineering attacks like phishing, take advantage of or rather target human vulnerabilities. In the post-pandemic world, adversaries keep employing these strategies, and while employees might be more aware today, threats are even more believable because threat actors can use Artificial Intelligence (AI) to craft an error free and convincing email. Organizations' training programs should cover cybersecurity awareness since this would assist the employees to identify threats and how to appropriately mitigate them. To minimize such risks, the actions as basic as realizing the phishing emails or as process as constituting the more complex passwords set an incredible impact [15]. A shortage of cybersecurity professionals is growing. Due to a shortage of qualified cybersecurity specialists, an increasing number of businesses are losing the fight against cyber threats. Due to the high number of threats, security teams become burned out and are not very effective in their desired tasks. Also, many small and medium-sized enterprises (SMEs) are unable to employ seasoned teams of cybersecurity professionals who would be able to mitigate threats posed to their organization. This leaves a gap that can only be filled by integrating Automation and Artificial Intelligence interventions to ease the challenges of threat detection and mitigation by the cybersecurity team [16-17].

3. AI role in Security Operations

3.1. Threat Detection, Incident Response, and Automation

Cybersecurity has taken a newer form and artificial intelligence is at the center of innovation. As the sophistication of cyber threats rises higher, companies are incorporating AI in an endeavor to increase security standards high. Machine learning and other AI technologies are increasingly used for threat identification, events handling and for automation which increases their speed, accuracy and efficiency. This section goes further to discuss how AI is implemented in these areas accompanied by further elaboration on its uses and value.

3.2. Artificial Intelligence role in Threat Detection

AI is capable of handling big data analysis in real time and therefore can pick early signs of a threat that may evade other systems from detection capabilities. There are lots of security alerts being generated by different applications daily for the cybersecurity team to analyze. Most of these alerts are false negatives, this can make the security professionals ignore genuine threats in the process. AI addresses this issue by accurately distinguishing between normal activities and focusing on high-risk occurrences. This capability allows cybersecurity teams to prioritize threats based on its impact [18-19]. In addition, AI technologies is able to detect zero-day vulnerabilities, advanced persistent threats, expose supply chain attacks and polymorphic malware that threats change often and may evade human detection. With artificial intelligence, processes such as log analysis, threat hunting, and compliance check are accomplished which alleviate the burden from analysts to deal with higher-order tasks, risk management, and planning [20-21].

3.3. Artificial Intelligence role in Threat Identification

Artificial intelligence improved threat detection by processing vast volumes of data in real time. Traditional security analysts use static rules to identify new security concerns, excluding new or complex threats. AI learns from the data and is far more successful at identifying the patterns of attacks than traditional systems, which depend on humans recognizing harmful activities [22]. AI are constantly scanning the traffic for any signs of anomaly in data packets or traffic in the overall network. This capability is very useful in threat recognition by preventing data exfiltration without proper authorization. AI is not limited to responding to set protocols, it is trained to understand what behaviors for a given network are normal and which are anomalous hence providing a prevention-based security solution [23-24].

3.4. Artificial Intelligence role in Identifying Unknown Threats

AI's most valuable role in cybersecurity is its capacity to detect zero-day vulnerabilities and completely new malware, respectively. These threats are substantially more detrimental since exploitation is based on a defect that engineers have not discovered or patched. Conventional security solutions fail to address such a threat mainly because they work by relying on existing threat signatures. While AI employs heuristic analysis and uses the concept of anomaly to discover malicious actors. AI is able to further identify new threats by observing how this threat vector interacts with files, external storage devices, memory, and system processes [25-26]. AI can also work with threat feeds to maintain information of the latest worldwide attack patterns. When incorporated with local network behavior, the AI system can learn possible attack angles and flag them [27].

3.5. AI's Role in Reducing False Alarms

Traditional security tools produce hundreds, if not thousands, of alerts daily. Most of the false alarms, which obscure actual threats and put pressure on security professionals. AI reduces this problem by offering much higher reliability of threat identification and minimizing false positives. This is realized using machine learning techniques where AI system has access to records on past alerts. It then can determine which of the patterns reflects actual threats and which are other activities that do not pose a threat [28]. AI can consider other factors, like if login correlates with the travel schedule, or whether MFA was involved, before classifying the alert as actionable. Not only does AI decrease false positives but it also eliminates situations when security teams grow tired due to numerous and often irrelevant alerts. This enhances security because all passive alarms are run to ground, leaving only real threats to warrant an investigation[29].

3.6. AI role in Improving Incident Response Times

AI improves the management of incidents by taking an important part of work that defines steps to prevent the continuation of the attack and minimize the impact of the attack for organizations. When AI identifies that a particular computer contains malware, AI can isolate the computer so as to stop lateral spread of the malware to other systems on the network. AI based incident response systems can provide detailed reports of threats that they have identified. Such

reports include the source of attack, the impacted systems and recommended actions. In this way, AI makes it possible for the security teams to make rational decisions immediately and avoid spending a lot of time on analysis. AI gives results regarding routine operations and threat intelligence allowing the cybersecurity professional to focus on decision making and planning [30-31].

3.7. AI role in Automating Repetitive Tasks and log analysis

Cybersecurity teams' workloads are always demanding given the many tasks that they must undertake. These tasks include patch management, log analysis, and access control, which are all repetitive. AI can perform these tasks with limited supervision and with less error. It is possible for the system to detect and sort out the risks depending on the impact and the likelihood that the threat will be exploited. It can then spread patches onto the affected systems, and guarantee that major vulnerabilities are remediate promptly. This automation is beneficial in so many ways besides time: It simply puts a limit to the amount of time attackers must enjoy themselves at a system with vulnerable vulnerabilities [32]. Security systems produce massive logs, and human analysts cannot, in any way, analyze all the logs they produce. The large logs generated can be managed by AI tools, where the tool analyses and find some patterns or irregularities, which are possibly security threats. AI makes sure that none of the relevant information is left out because the procedure occurs automatically [33].

4. Post-Pandemic Vulnerabilities

COVID-19 significantly impacted the lifecycle of organizations by drastically altering the way companies operate around the world and embrace remote work as well as cloud platforms. As these changes have allowed continuous business operation, they have also prompted a number of new cybersecurity risks.

4.1. Expanded Attack Surface

There is no doubt that the transition to remote work expanded the organizations' attack surface. In the pre COVID-19 office arrangements, different organizations' networks and appliances were confined and safeguarded in enclosed organizations. Remote work meant that while conducting activities employees were connecting to the company's resources over the internet using their own devices and networks that do not possess the same level of protection as enterprise ones [34]. Unlike Corporate Owned Business Only (COBO) devices, most personal devices are not updated with the current security features. Policies should be made that restrict employees from accessing organization network from devices that are not approved by the information technology team [35-36]

4.2. Increased dependency on Cloud-Based Services

The use of cloud solutions increased significantly during the pandemic, when companies needed tools that enable and support work on the internet. Cloud services allow businesses to operate online, but they have inherent security vulnerabilities that need to be fixed. Cloud has risks such as weak access control configuration which could allow attackers gain unauthorized access to data or launch attacks on the organization's networks [37]. Also, cloud solutions depend on using APIs as the default way to integrate applications and services . These APIs are yet again vulnerable and if exploited, can act as an entry point for any attacker into the organization network. Malicious actors can launch an attack against a system through insecurity coding practices in the API development. To mitigate this risk, organizations must conduct security assessments continually, while APIs to be established should be with secure coding [38].

4.3. Weak Authentication and Access Controls

Remote work brought into practice the use of remote access technologies like VPNs, Remote Desktop Protocols (RDP), communication software like Teams, Slack etc. Despite the benefits of this tools in promoting effective communication and work, they create a gateway for the attackers especially when the authentication controls are inadequate. Even today, most organizations continue to rely on old security technologies such as password-based authentication, which clearly cannot cope with current threats. Passwords are commonly reused, easy to remember and prone to brute force attacks. Hackers use stolen credentials to conveniently get into critical systems raising the risk of data leakage or ransomware infection [39-40].

The absence of effective access control to such a system only aggravates the situation. Often employees are given access privileges higher than their working responsibilities to carry out, and this makes the company's resources vulnerable to either misuse or intentional abuse. To counter these concerns organizations should implement policies that ensure that employees have only the minimum required permissions to perfect tasks assigned to them. Organizations should have password policies that include password length and prevent reuse of the same passwords on different accounts [41].

4.4. Increased Social Engineering and Phishing Attacks

As work becomes more remote, phishing and social engineering have become more effective. Friends, colleagues, clients, and partners interact through emails, chats and video conferencing making it easier for hackers to trick them. Phishing attacks are much more refined and faked e-mails are sent to people with the intent of encouraging the user to enter their login details or follow links to a fake website. They are now also occurring in chat apps like Slack, in which a cracker pretends to be a team member and requests documents or monetary data. To safeguard against such threats, organizations must train employees with simulated phishing attacks and provide feedback. Also, the IT team should implement email safety measures that is capable of detecting suspicious links, attachments and senders [42]

5. Conclusion

The pandemic has influenced the evolution of digital space and opened new possibilities and threats to cybersecurity. The swift transition to remote work and adoption of cloud services increased exposure to threats. artificial intelligence has become crucial in increasing the quality of threat identification, as well as automating the responses. These tools supported the demand for robust data management and compliance with the necessary ethical standards. The study goes beyond technological solutions, and it underscores that the cybersecurity skills gap needs to be addressed, organizational policies strengthened, and the collaboration among businesses, governments and researchers globally must be promoted. Emerging threats will become more and more sophisticated, and it is increasingly important for us to adopt proactive strategies, ethical integration of emerging technologies, and evolve defenses in a continuous way to address future challenges.

Compliance with ethical standards

Disclosure of conflict of interest

The authors claim that there is no conflict of interest.

References

[1] Choudhary, A., Choudhary, G., Pareek, K., Kunndra, C., Luthra, J., and Dragoni, N. Emerging cyber security challenges after COVID pandemic: a survey. Journal of Internet Services and Information Security. (2022); 12(2), 21-50.

[2] Ahmad, T. Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. 2020; Available at SSRN 3568830

[3] Holovkin, B. M., Tavolzhanskyi, O. V., and Lysodyed, O. V. Corruption as a cybersecurity threat in conditions of the new world's order. Linguistics and Culture Review. 2021; 5(S3), 499-512.

[4] Reshmi, T. R. Information security breaches due to ransomware attacks-a systematic literature review. International Journal of Information Management Data Insights. 2021; 1(2), 100013.

[5] Rizvi, S., Orr, R. J., Cox, A., Ashokkumar, P., and Rizvi, M. R. Identifying the attack surface for IoT network. Internet of Things. 2020; 9, 100162.

[6] Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., and Díaz-Castaño, N. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies. 2021; 23(sup1), S47-S59.

[7] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., and Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and security. 2021; 105, 102248.

[8] Hawdon, J., Parti, K., and Dearden, T. E. Cybercrime in America amid COVID-19: The initial results from a natural experiment. American Journal of Criminal Justice. 2020; 45(4), 546-562.

[9] Plachkinova, M. Exploring the Shift from Physical to Cybercrime at the Onset of the COVID-19 Pandemic. International Journal of Cyber Forensics and Advanced Threat Investigations. 2021; 2(1), 50-62.

[10] Neeley, T. Remote work revolution: Succeeding from anywhere. London, UK: Harper Business; 2021

[11] Popovici, V., and Popovici, A. L. Remote work revolution: Current opportunities and challenges for organizations. Ovidius Univ. Annual Economics Sciences Series. 2020; 20(1), 468-472.

[12] Pranggono, B., and Arabo, A. COVID-19 pandemic cybersecurity issues. Internet Technology Letters. 2021; 4(2), e247.

[13] Lang, M., Connolly, L., Taylor, P., and Corner, P. J. The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks. Digital Threats: Research and Practice. 2023; 4(4), 1-22.

[14] Gero, S., Back, S., LaPrade, J., and Kim, J. Malware infections in the US during the COVID-19 pandemic: an empirical study. International Journal of Cybersecurity Intelligence and Cybercrime. 2021; 4(2), 25-37.

[15] Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., and Bonacina, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors. 2021; 21(15), 5119.

[16] Crumpler, W., and Lewis, J. A. Cybersecurity Workforce Gap (p. 10). Center for Strategic and International Studies (CSIS); 2022

[17] DeCrosta, J. Bridging the Gap: An Exploration of the Quantitative and Qualitative Factors Influencing the Cybersecurity Workforce Shortage (Master's thesis, Utica College); 2021

[18] Yaseen, A. AI-driven threat detection and response: A paradigm shift in cybersecurity. International Journal of Information and Cybersecurity. 2023; 7(12), 25-43.

[19] Chakraborty, C., and Abougreen, A. Intelligent internet of things and advanced machine learning techniques for COVID-19. EAI Endorsed Transactions on Pervasive Health and Technology. 2021; 7(26).

[20] Rizvi, M. Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. International Journal of Advanced Engineering Research and Science. 2023; 10(05)

[21] Reddy, A. R. P. The Role of Artificial Intelligence in Proactive Cyber Threat Detection In Cloud Environments. NeuroQuantology. 2021; 19(12), 764-773.

[22] Maddireddy, B. R., and Maddireddy, B. R. Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment. International Journal of Advanced Engineering Technologies and Innovations. 2020; 1(2), 64-83.

[23] Nina, P., and Ethan, K. AI-Driven Threat Detection: Enhancing Cloud Security with Cutting-Edge Technologies. International Journal of Trend in Scientific Research and Development. 2019; 4(1), 1362-1374.

[24] Raza, H. Proactive Cyber Defense with AI: Enhancing Risk Assessment and Threat Detection in Cybersecurity Ecosystems; 2021

[25] Beshwari, F., Beshwari, M., and Beshwari, A. The Role of Artificial Intelligence in Mitigating Unknown-Unknown Risks. The Role of Artificial Intelligence in Mitigating Unknown-Unknown Risks. 2020; 64(1), 13-13.

[26] Wood, S. Artificial Intelligence Applications for Solving Combat Identification Problems Concerning Unknown Unknowns (Doctoral dissertation, Monterey, CA; Naval Postgraduate School); 2019

[27] Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., and Tatarchenko, Y. The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. Economic Affairs. 2024; 69, 43-51.

[28] Adeosun OA, Fakeyede MO, Adesola, AA, Akingbulere G and Anifowoshe DO. Security Implication of network slicing in 5g-Enabled IoT environment. World Journal of Advanced Research and Reviews. 2024; 24(03)2359-2373.

[29] Nybø R, Bjørkevoll KS, Rommetveit R. Spotting a False Alarm—Integrating Experience and Real-Time Analysis With Artificial Intelligence. InSPE Intelligent Energy International Conference and Exhibition 2008 Feb 25 (pp. SPE-112212). SPE.

[30] Li, B., Yue, L., Nie, H., Cao, Z., Chai, X., Peng, B. and Huang, W. The effect of intelligent management interventions in intensive care units to reduce false alarms: An integrative review. International Journal of Nursing Sciences. 2024; 11(1): 133-142.

[31] Liu, W. C., Lin, C., Lin, C. S., Tsai, M. C., Chen, S. J., Tsai, S. H., and Cheng, C. C. An artificial intelligence-based alarm strategy facilitates management of acute myocardial infarction. Journal of Personalized Medicine. 2021; 11(11): 1149.

[32] Eziefule, A. O., Adelakun, B. O., Okoye, I. N., and Attieku, J. S. The Role of AI in Automating Routine Accounting Tasks: Efficiency Gains and Workforce Implications. European Journal of Accounting, Auditing and Finance Research. 2022; 10(12): 109-134.

[33] Au-Yong-Oliveira, M., Canastro, D., Oliveira, J., Tomás, J., Amorim, S., and Moreira, F. The role of AI and automation on the future of jobs and the opportunity to change society. In New Knowledge in Information Systems and Technologies: 2019; 3:348-357.

[34] Ammaturo, P., Ammaturo, C., Letizia Fallucca, M. B., and Aiello, P. Challenges to the Inclusion of Vulnerable Social Groups in Pandemic and Post-Pandemic Society. Social Work Review/Revista de Asistenta Sociala. 2023; (1).

[35] Leach, M., MacGregor, H., Scoones, I., and Wilkinson, A. Post-pandemic transformations: How and why COVID-19 requires us to rethink development. World development. 2021; 138: 105233.

[36] Pele A, Riley S. Vulnerability, Biopolitics, and Political Struggles: Some Thoughts on (Post) pandemic Times. Law, Culture and the Humanities. 2025; 21(1):4-6.

[37] Van Der Vlist, F., Helmond, A., and Ferrari, F. Big AI: Cloud infrastructure dependence and the industrialization of artificial intelligence. Big Data and Society. 2024; 11(1): 205

[38] Chanthati, S. R. Artificial Intelligence-Based Cloud Planning and Migration to Cut the Cost of Cloud Sasibhushan Rao Chanthati. American Journal of Smart Technology and Solutions. 3(2), 13-24.

[39] Kommisetty, P. D. N. K., and Nishanth, A. (2024). AI-Driven Enhancements in Cloud Computing: Exploring the Synergies of Machine Learning and Generative AI; 2024.

[40] Tellabi, A., Sassmanhausen, J., Bajramovic, E., and Ruland, K. C. Overview of Authentication and Access Controls for IandC systems. In 2018 IEEE 16th International Conference on Industrial Informatics (INDIN); 2018; 882-889.

[41] Mahalle, P. N., Anggorojati, B., Prasad, N. R., and Prasad, R. Identity authentication and capability-based access control (IACAC) for the internet of things. Journal of Cyber Security and Mobility. 2013; 1(4): 309-348.

[42] Omotunde, H., and Ahmed, M. A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. Mesopotamian Journal of CyberSecurity. 2023; 115-133.