A Review of Cybersecurity Challenges in the Post-Pandemic World

Adeyemi Afolayan Adesola,[†], Awele Mary-Rose Ilusanmi [††]

[†]Computer science Department, Stephen F. Austin State University, Nacogdoches, Texas, USA
[††]College of Arts and Liberal Arts, Stephen F. Austin State University, Nacogdoches, Texas, USA

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. To defend against these emerging 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 review highlight AI can adapt dynamically to curbing existing risks, perform effective optimization of repetitive tasks, analyze polymorphic virus and help in minimizing burden on a cybersecurity team who can focus on decision making and risk prevention. This study further shows how the application of AI can fill still existing cybersecurity workforce deficiency and improve security in various spaces ranging from working from home environments to cloud environments. This review also highlights the impact of post pandemic vulnerabilities such as expanded attack surface, increased dependency on cloud-based services, weak encryption and social engineering attacks.

Keywords:
Polymorphic virus, post pandemic vulnerabilities, Social engineering, Artificial intelligence

1. Overview of Cybersecurity Challenges in the Post-Pandemic World

COVID-19 influenced the global digital environment drastically changing the dynamics of the entire world and offering situations that none 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 lock down and practicing physical social distance. However, this extremely 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 had increased because 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 phishers designed their messages and approached their intended targets increased, 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 a 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].

Objectives of this study

This research can help to review how the evolution of cybersecurity occurred after the COVID-19 pandemic and how emerging technologies, including AI, contribute to mitigating threats. Therefore, this review provides an understanding of the existing and future state of cybersecurity by observing how the pandemic disrupted it

Manuscript received January 5, 2026
Manuscript revised January 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.1.15

and in what ways AI applications assist with threat identification and management.

2. The Surge in Cybercrime

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],[8],[9].

The Remote Work Revolution

The outbreak of COVID19 led to new changes in people’s working conditions, and one of the most significant changes was remote work. While this helped business 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. Most employees were connecting to secure internal networks through unsecure Wi-Fi, personal devices that lack strong encryption. These weaknesses were seized by cybercriminals within a short time. For instance, they 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].

Digital Transformation on the Spotlight

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. Many businesses started to use cloud services, collaborative tools and e- commerce facilities without knowing the insecurity factors or without adequate protection.

Challenges in Cloud Security

There has been a massive increase in adoption of cloud services due to the pandemic as business required 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 and Its Evolution

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]

The Human Factor

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].

The Stress on Cybersecurity Professionals

Cybersecurity skills professional’s deficit is on the rise. More and more companies lose the battle to cyber threats due to the lack of skilled cybersecurity professionals. 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 size 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: Threat Detection, Incident Response, and Automation

Cybersecurity has taken on a newer twist, and artificial intelligence is at the center of the innovation. As the sophistication of cyber threats rises higher, companies are incorporating in 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.

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 mitigates this problem by providing accurate differentiation of benign activities and focusing on high-risk events. 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].

Artificial Intelligence role in Threat Identification

Through analyzing large amounts of data in real-time, the use of AI enhanced threat identification. Analysts of traditional security tools utilize static rules in identifying new security threats which exclude new or complex threats. While traditional methods rely on human recognition of malicious activity, AI evolves from the data and is significantly more effective for the identification of the attack's patterns [22]. AI systems of a network system 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 due permission. 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].

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 relatively more lethal since the exploitation is made from a flaw that has not been recognized or patched by engineers. 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 latest worldwide attack patterns. When incorporated with local network behavior, the AI system can learn possible attack angles and flag them [27].

Artificial Intelligence Role in Reducing False Alarms

Traditional security tools produce hundreds, if not thousands, of alerts daily. The majority of them are 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 take into account 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].

AI role 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 a particular computer that 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].

4. 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 likelihood that the threat will be exploited. It can then spread patches onto the affected systems, and guarantee that major vulnerabilities are remediated promptly. This automation is beneficial in so many ways besides time: It simply puts a limit to the amount of time attackers have to enjoy themselves in 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 finds 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].

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 allowed the continuous business operation, they have also prompted a number of new cybersecurity risks.

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]

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 to 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 have to conduct security assessments continually, while APIs to be established should be with secure coding [38].

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 these 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].

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 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 have 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 collaboration among businesses, governments and researchers globally must be promoted. Emerging threats will become increasingly 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.

Method

This examines the impact of AI on cybersecurity practices in the post pandemic era. It was done by analyzing reports from the industry, academic papers, and threat reports gathered from across the world to determine trends in the use of AI in threat modeling, threat response, and automation.

Conflict of interest

There is no conflict of interests

Research Implications

This research highlights the need for proactive application of AI in cybersecurity due to its prospects for improving threat identification, time response, and organizational performance.

References

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

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

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

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

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

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

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

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

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

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

[11] Popovici, V., & Popovici, A. L. (2020). Remote work revolution: Current opportunities and challenges for organizations. Ovidius Univ. Ann. Econ. Sci. Ser, 20(1), 468-472.

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

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

[14] Gero, S., Back, S., LaPrade, J., & Kim, J. (2021). Malware infections in the US during the COVID-19 pandemic: an empirical study.

International Journal of Cybersecurity Intelligence & Cybercrime, 4(2), 25-37.

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

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

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

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

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

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

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

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

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

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

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

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

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

[28] Lee, D., Lai, C. W., Liao, K. K., & Chang, J. W. (2021). Artificial intelligence assisted false alarm detection and diagnosis system development for reducing maintenance cost of chillers at the data centre. Journal of Building Engineering, 36, 102110.

[29] Nybø, R., Bjørkevoll, K. S., & Rommetveit, R. (2008, February). Spotting a False Alarm—Integrating Experience and Real-Time Analysis With Artificial Intelligence. In SPE Intelligent Energy International Conference and Exhibition (pp. SPE-112212). SPE.

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

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

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

[33] Au-Yong-Oliveira, M., Canastro, D., Oliveira, J., Tomás, J., Amorim, S., & Moreira, F. (2019). 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: Volume 3 (pp. 348-357). Springer International Publishing.

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

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

[36] Pele, A., & Riley, S. (2024). On Vulnerability, Biopolitics, and Political Struggles: Some Thoughts on (Post) pandemic Times. Law,

Culture and the Humanities, 17438721241269429.

[37] van der Vlist, F., Helmond, A., & Ferrari, F. (2024). Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. Big Data & Society, 11(1), 20539517241232630.

[38] Chanthati, S. R. (2024). 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., & Nishanth, A. (2024). AI-Driven Enhancements in Cloud Computing: Exploring the Synergies of Machine Learning and Generative AI.

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

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

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

Adeyemi Adesola received the MSc in Cyber Security from Stephen F. Austin State University, Nacogdoches, Texas, USA in May 2024. Adeyemi Adesola is a cybersecurity professional with experience in vulnerability assessment and penetration. He has consulted for SMEs in Nigeria. He holds a Master of Science Degree in Cybersecurity from Stephen F. Austin State University, Nacogdoches, Texas. Adeyemi has certification in CompTIA Security+ and Certified in Cybersecurity from (ISC)2. He also owns his own blog (yemiadesola.com) where he shares insights with millions of readers around the world. He also writes for journals and national newspapers. Adeyemi is a member of two renowned cybersecurity association namely Information Systems Audit and Control Association (ISACA) and Information Systems Security Association (ISSA).

Awele Ilusanmi received a Master Degree in Liberal Arts. Awele Ilusanmi is a Information Security Awareness for kids advocate, a distinguished author and a multiple award-winner, celebrated for her invaluable support and contributions to the Nigerian literary landscape. She is an extremely passionate literacy advocate. She was a speaker and panelist at the 2019 Edition of Connect Nigeria's Writers' Conference on the topic “Successful Book Marketing" and a Panelist at the Lagos Books and Art Festival (LABAF) 2023. At LABAF 2023, she shared her expertise on the topic "Winning with Book Publishing and Marketing”. She is passionate about seeing authors succeed and writes books on Book Marketing Strategies and Promotions to share her experience and knowledge freely. Awele Ilusanmi is the President of Literary Authors Cooperative Multipurpose Society of Nigeria and Founder of Book Marketing Class Africa BMACA. Awele Ilusanmi is a Literary Agent with Publishizer, an award-winning Literary Crowdfunding Company in New York, USA. She is also the Author of Book Marketing Strategies, Comforting Arms, Launch Money and Profitable Pages. Awele Ilusanmi is a graduate of Publishing Studies from the Stephen F Austin State University, Nacogdoches, Texas, USA. She was the keynote speaker at an event organized by Booksellers Association of Nigeria on 17th October 2024 and spoke on: “Creative, Innovative, and Aggressive Marketing Approaches for selling more books”. Awele Ilusanmi was a panelist at the highly anticipated Writers Interactive Network Literary Festival 3 tagged ARTSLIVELAGOS on 16th November 2024. She spoke on Book PR for the 21st Century. As a testament to her excellence and impact, Awele Ilusanmi has been awarded the African Writers Tribe Transformational Leader Award 2025; The Trinity Writers and Publishers Network Award for Excellence in Education and Rotary Club of Ikate, Nigeria's humanitarian award for her contribution to child literacy and youth development. Awele has a passion for literary accomplishments and only sees possibilities when faced with challenges and difficulties.