Migration Letters

Volume: 20, No: S9(2023), pp. 1066-1072

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection: A Comprehensive Review

Fanar Shwedeh[1], Sawsan Malaka[2], Bushra Rwashdeh[3]

Abstract

Artificial Intelligence vs. Human Expertise in cybersecurity is a big challenge, as human experts play a critical role in fending off threats generated by AI. AI-driven technologies in conjunction with human analysts can provide a more thorough defending plans against complex attacks. This article examines how AI hackers impact the relationship between organization's cyber security conducts and the sustainability of software protection in these organizations. 50 interviews and open-end surveys were distributed to cybersecurity specialists in Dubai, United Arab Emirates (U.A.E.). The findings of the statistics show different observations. A moderation effect of artificial intelligence hackers is appearing to have a positive moderating influence on the relationship of cybersecurity conducts and sustainability of software protection. A negative moderation on the other hand is found where AI hackers may find ways to exploit security flaws and continuously adapt in order to negatively moderate the relationship. This might weaken software protection's sustainability and make it harder to keep up with new threats. As a significance of this study, it is strongly recommended to implement robotics monitoring mechanisms and develop security lifecycles which are found to be crucial. Organizations need to spend more money on cutting-edge cyber security procedures and improving the long-term viability of their software protection.

Keywords: *Cybersecurity, AI Hackers, AI, Sustainability, Software Protection, Security Conducts.*

Introduction

What if AI is used as a tool of a negative manner? Within the field of cybersecurity, one of the most important and rapidly developing area of research is the use of Artificial Intelligence as AI hackers on the relationship between software protection and cyber security practices. Organizations must comprehend and lessen the effects of AI hackers if they hope to preserve strong software security against ever more advanced threats (Tabrizchi et al., 2020; Khadragy et al., 2022). In this review, the sustainability of software protection is examined under the risk of AI hackers with consideration to the applied cybersecurity conducts in the investigated organizations (Tabrizchi et al., 2020; Müssig et al., 2021; Salloum et al., 2023). The relationship between software protection and cybersecurity practices is moderated by the existence of AI hackers, as it increases the demand for defence mechanisms that are more sophisticated, flexible, and AI-driven

[1] Assistant Professor, City University Ajman, Ajman, UAE, s.fanar@cu.ac.ae
[2] PhD Researcher, Computer Science College, British University in Dubai, Dubai, UAE, 22000950@student.buid.ac.ae
[3] PhD Researcher, Computer Science College, British University in Dubai, Dubai, UAE, 22000643@student.buid.ac.ae

(Aljumah et al., 2020; Ravikumar et al., 2022; Shwedeh et al., 2022a). This necessitates a flexible approach to cybersecurity, combining human knowledge and AI technologies to successfully protect software systems. 50 interviews were conducted with Cybersecurity specialists in different companies in the UAE. They stated that no matter what codes of conducts and cybersecurity systems are applied, they can never guarantee certain and sustainable protection of their systems. AI has no limitations to its power, and this can be considered as the first challenge for these specialists. Many systems are recognizing the AI hackers but as they are unlimited, the protection stability gets uncertain (Müssig et al., 2021).

Artificial Intelligence Hackers

In the context of cybersecurity, artificial intelligence (AI) can be applied both offensively and defensively. The concept of "Artificial Intelligent Hackers" is referring to the way malevolent actors use AI to improve their capacity for hacking and cyberattacks (Shamiulla et al., 2019). Here are some important things to think about Cyberattacks which are powered by AI such as Malevolent actors who can automate and enhance different phases of a cyberattack by utilizing AI and machine learning techniques. This covers activities like reconnaissance, vulnerability identification, exploiting, and detection avoidance. Phishing and Social Engineering is and Artificial Intelligence which has the potential to create more realistic social engineering and phishing emails. AI can assist attackers in crafting highly personalized and targeted messages to trick people by analysing large amounts of data. Malware and malicious code are also a type of (AI) that can be used to create more complex and evasive malware (Ma et al., 2020). AI can be used, for instance, to create polymorphic malware, which modifies its code to evade detection through signatures. Automated vulnerability scanning can be used to continuously check systems and networks for vulnerabilities (Li et al., 2020). As a result, attackers can quickly find and take advantage of vulnerabilities. Evasion and Intrusion Detection is applied defensively to improve intrusion detection systems, increasing the difficulty of an attacker's network infiltration (Khraisat et al., 2019; Li et al., 2020). AI can be used offensively to create evasion strategies that get beyond these detection systems. Autonomous Botnets attackers may be able to construct autonomous botnets with AI that can modify their strategies and behaviour in reaction to shifting conditions. This increases the difficulty of opposing them. As an addition, data Exfiltration attackers can steal important information covertly by using artificial intelligence (AI) to analyse and exfiltrate sensitive data more effectively (Li et al., 2020; Sabir et al., 2021; Shwedeh et al., 2022b; Alkashami et al., 2023). AI can expedite the password cracking process by identifying patterns and frequently used password structures. Attackers will find it simpler to obtain unauthorized access to accounts and systems as a result (Khraisat et al., 2019; Li et al., 2020).

It takes a combination of cutting-edge AI-based security solutions and conventional cybersecurity measures to defend against hackers who use artificial intelligence (Kaur et al., 2019). This includes real-time threat identification and response capabilities provided by machine learning algorithms, behaviour analysis, and anomaly detection (Kaur et al., 2019; Sabir et al., 2021; Abdallah et al., 2022; Aburayya et al., 2023). It is imperative for organizations to guarantee that their workforce is adequately trained to identify and counteract AI-powered assaults, like intricate phishing schemes. It's critical to remember that there are drawbacks in using AI in cybersecurity. The use of AI for malevolent intent raises important ethical and legal issues, even though it can improve the skills of both attackers and defenders (Jobin et al., 2019). To address these issues and lessen the risks connected to hacking powered by AI, governments, organizations, and the cybersecurity community are collaborating to create rules, guidelines, and best practices (Kaur et al., 2019; Li et al., 2020; Sabir et al., 2021).

Cybersecurity conducts

Cybersecurity is the process of defending computer networks, systems, and data against different types of threats, such as malware, illegal access, data breaches, and other cyberattacks (Shamiulla et al., 2019; Ma et al., 2020). To protect digital assets and guarantee the confidentiality, integrity, and accessibility of information, cybersecurity procedures and measures must be followed (Miric et al., 2019; Shwedeh et al., 2020). There are many crucial cybersecurity behaviours that can help in protecting software systems from harmful security challenges and threats. Risk assessment is used to find possible weak points and dangers in the digital infrastructure of your company, do frequent risk assessments (Miric et al., 2019; Shamiulla et al., 2019; Ma et al., 2020; Shwedeh, F. 2024). Strong access control procedures should be put in place to guarantee that only people with permission can access sensitive information and systems. Network Security is the use intrusion detection and prevention systems, firewalls, and encryption to safeguard your network infrastructure from outside threats (Priyadarshini, I. 2019). Patch Management applies security patches and updates to operating systems, applications, and software to keep them current and reduce known vulnerabilities (Priyadarshini, I. 2019; Ma et al., 2020; Salameh et al., 2022). Employee Education and training staff members on social engineering awareness, strong password management, and phishing email detection as well as other cybersecurity best practices is essential. Component Security testing and code review to find and address security flaws depends on employees and cybersecurity specialists who create a thorough incident response plan to quickly address and mitigate cyber incidents (Priyadarshini, I. 2019; Shamiulla et al., 2019; Ma et al., 2020; Shwedeh et al., 2023). This is considered as a part of security awareness to encourage staff to report questionable activities, cultivate a culture of cybersecurity awareness within your company. Require the use of multi-factor authentication (MFA) to add an extra security layer when gaining access to accounts and sensitive systems. Data Encryption is a part of the conducts to prevent unwanted access, encrypt critical data while it's in transit and at rest (Müssig et al., 2021; Sabir et al., 2021). Frequent Backups makes sure that routinely backup for important data is active, to enable speedy recovery if cyberattacks cause data loss. Endpoint Security is used as well to guard against malware and other threats, use antivirus software, intrusion detection systems, and other security measures on individual devices (Priyadarshini, I. 2019; Sabir et al., 2021; Ravikumar et al., 2023). Cybersecurity specialists use secure coding to create and manage safe software and applications by adhering to best practices, which reduce vulnerabilities. Vendor Management verifies that partners and vendors of cybersecurity procedures adhere to the security guidelines by evaluating them. Data privacy settings make sure that employee and customer data is private by adhering to applicable data protection regulations. Monitoring and logging are also used to identify and address security incidents, put in place reliable monitoring and logging systems. Business communication through managements should be secure communication (Sabir et al., 2021; Shwedeh et al., 2021; Yaacoub et al., 2021). When sending data over the internet, encrypted communication protocols like HTTPS and Mobile Device Management (MDM). Using MDM programs will enhance safeguard and control mobile devices used by employees at organizations (Odun-Ayo et al., 2019; Ma et al., 2020).

Sustainability of Software protection

The long-term viability and efficacy of safeguards put in place to prevent software from unauthorized access, copying, modification, or distribution are referred to as sustainability of software protection (Aljumah et al; 2021). For software developers and organizations to safeguard their intellectual property, guarantee revenue streams, and preserve the integrity of their products, sustainability of software protection is a crucial factor (Miric et al., 2019; Shamiulla et al., 2019; Nishant et al., 2020). There are many elements that should be taken into account when evaluating the sustainability of software

protection. Constant Updates are needed to guard against changing threats and vulnerabilities, software protection mechanisms need to be updated on a regular basis. Patches and updates should be created and released whenever new security vulnerabilities are found in the software to keep it safe (Aljumah et al; 2021). Strong Encryption is one of the most important aspects of software protection is encryption. To keep the software secure, it is essential to make sure the encryption is robust and current. Software distribution and unauthorized use can be avoided by putting in place efficient licensing and activation procedures. Updating these systems can increase their efficacy and help them adjust to changing conditions (Miric et al., 2019; Aljumah et al; 2021). Code obfuscation where attackers can find it more challenging to decipher and comprehend the software's source code when utilizing obfuscation techniques. It's crucial to update and enhance obfuscation techniques on a regular basis (Tabrizchi et al., 2020; Müssig et al., 2021). Safe Key Management works based on cryptographic keys and other security credentials must be handled carefully. It's critical to follow best practices and maintain up-to-date key management systems because inadequate key management can result in vulnerabilities. Digital rights management (DRM) is one example of an anti-piracy measure that can be used to prevent unauthorized software distribution and copying (Garba et al., 2021; Tabrizchi et al., 2020; El Nokiti et al., 2022). For these precautions to remain ahead of pirate strategies, they should be continuously enhanced. User Education is an essential way to promote sustainability by teaching users the value of using authorized software and the dangers of using cracked or pirated versions. As an addition, Legal Enforcement which is implemented by taking software pirates and counterfeiters to court can serve as a deterrent (Miric et al., 2019; Nishant; 2020; Dahu et al., 2023). To detect and resolve infringement, this method necessitates constant work. Many cybersecurity specialists, whom we interviewed, revealed that their organizations have collaboration with Security Experts. That help in keeping protection mechanisms current with the newest threats and that can be achieved by collaborating with cybersecurity experts and organizations that are specialize in software protection. Redundancy and Defence in Depth is another procedure in sustaining software protection. Using defence in depth, or layering security measures, can improve sustainability. Combining different security measures increases the difficulty of software compromise for attackers. There are also frequent security audits that have regular security auditors and vulnerability assessments which can assist in detecting AI hackers and quickly fixing software protection flaws.

Findings:

30% of the organizations that is, 15 out of 50, stated that they are having a mixture of the previous cyber security conducts. The remaining 35 organizations, which are 70% of the sample, are organizations that are using monitoring and incident response systems. They put in place incident response procedures and monitoring systems to identify illegal access or tampering guarantees that security breaches can be promptly fixed. These 50% organizations have legal and regulatory compliance. Their objective is to focus is on maintaining software protection over the long term which depends on adhering to pertinent laws and regulations, such as those pertaining to copyright and intellectual property rights. They also include user feedback and bug reporting. By encouraging users to report bugs and vulnerabilities in the software, security measures can be improved, and potential threats can be addressed. Software protection sustainability is a continuous process that calls for attention to detail and adjustment to evolving threats and technological advancements. To protect their products and intellectual property over time, software developers and organizations must make security and protection measures investments.

Discussion:

An open-end survey was distributed the 50 cybersecurity specialists to investigate how to sustain software protection in Dubai organizations under the risk of AI hackers with consideration to their current cybersecurity conducts. Employing Strong Encryption is one proposed solution to safeguard sensitive data in organizations. Using strong encryption algorithms by updating and patching encryption libraries frequently was examined to fix security flaws. The examined encryptions in our study included three main results:

1- Secure Development Lifecycle (SDLC): As operations managers design products life cycles for their products and services, Secure Development Lifecycle (SDLC) is strongly recommended to be developed in organizations. The results of the open-end surveys show that SDLC positively influences the sustainability of software protection in organizations under the risk of AI hackers. Planning and designing SDLC can be through coding and testing, all stages of the software development lifecycle and that will detect the decline of the cybersecurity systems once it lacks.

2- Threat Modelling: The open-end surveys resulted in showing no impact on the sustainability of software protection. Possible security risks and weaknesses that might be unique to the software might not be able to detect the unlimited of AI hackers used in the threat modelling.

3- Implementing robotics monitoring mechanisms: AI cybersecurity systems are founded be strongly enhancing the sustainability of software protection against AI hackers. The result of the open-end survey reflects that implementing robotics monitoring mechanisms in organizations can detect and respond to AI security incidents in real-time even if these incidents are not identified in applied cybersecurity built-in systems.

Conclusion

Cybersecurity practices are applied by different strategies, policies, and actions that companies take to safeguard their data and software against online threats. Sustainability of software protection is stable as long as the security measures implemented on software and systems are resilient and effective over the long run. Sustainability of software protection concerns the degree to which a software system can tolerate changing threats and adjust to them over time. Artificial Intelligence Hackers in this study context is examined as a moderator to analyse the effect of using machine learning and artificial intelligence by malevolent actors to conduct automated and highly skilled cyberattacks. These AI-driven attacks are especially difficult to defend against because of their quick evolution and adaptability. Complex Interaction shows that depending on the particular security procedures put in place by organizations, the hackers' AI capabilities, and other external circumstances, the relationship between AI hackers and organizations may be more complex. Ongoing Enhancement is needed to keep up with the latest security best practices and emerging threats. As new problems arise, developing security lifecycles and implementing robotics monitoring mechanisms as AI software protection techniques is essential. Continuous vigilance and a dedication to security are necessary for sustainable software protection. To ensure the long-term security of software in organizations, it is imperative that cybersecurity specialists establish an AI culture of security within the cybersecurity development teams and organization systems.

References

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET communications, 14(7), 1185-1191.

Müssig, S., Reichstein, J., Prieschl, J., Wintzheimer, S., & Mandel, K. (2021). A Single Magnetic Particle with Nearly Unlimited Encoding Options. Small, 17(28), 2101588.

Shamiulla, A. M. (2019). Role of artificial intelligence in cyber security. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4628-4630.

Ma, Z., Ge, H., Wang, Z., Liu, Y., & Liu, X. (2020). Droidetec: Android malware detection and malicious code localization through deep learning. arXiv preprint arXiv:2002.03594.

Li, X., Wang, L., Xin, Y., Yang, Y., & Chen, Y. (2020). Automated vulnerability detection in source code using minimum intermediate representation learning. Applied Sciences, 10(5), 1692.

Sabir, B., Ullah, F., Babar, M. A., & Gaire, R. (2021). Machine learning for detecting data exfiltration: A review. ACM Computing Surveys (CSUR), 54(3), 1-47.

Kaur, J., & Gill, N. S. (2019). Artificial Intelligence and deep learning for decision makers: a growth hacker's guide to cutting edge technologies. BPB Publications.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature machine intelligence, 1(9), 389-399.

Miric, M., Boudreau, K. J., & Jeppesen, L. B. (2019). Protecting their digital assets: The use of formal & informal appropriability strategies by App developers. Research Policy, 48(8), 103738.

Priyadarshini, I. (2019). Introduction on cybersecurity. Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies, 1-37.

Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems, 77, 103201.

Nishant, R., Kennedy, M., & Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. International Journal of Information Management, 53, 102104.

Garba, A., Dwivedi, A. D., Kamal, M., Srivastava, G., Tariq, M., Hasan, M. A., & Chen, Z. (2021). A digital rights management system based on a scalable blockchain. Peer-to-Peer Networking and Applications, 14, 2665-2680.

Salloum, S., Al Marzouqi, A., Alderbashi, K. Y., Shwedeh, F., Aburayya, A., Al Saidat, M. R., & Al-Maroof, R. S. (2023). Sustainability Model for the Continuous Intention to Use Metaverse Technology in Higher Education: A Case Study from Oman. Sustainability, 15(6), 5257.

Shwedeh, F.,Hami, N., Abu BakarS., Mat Yamin, F., Anuar, A. (2022a). The Relationship between Technology Readiness and Smart City Performance in Dubai. Journal of Advanced Research in Applied Sciences and Engineering Technology, 29(1), 1–12. https://doi.org/10.37934/araset.29.1.112

Aburayya, A., Salloum, S., Alderbashi, K., Shwedeh, F., Shaalan, Y., Alfaisal, R., Malaka, S & Shaalan, K. (2023). SEM-machine learning-based model for perusing the adoption of metaverse in higher education in UAE. International Journal of Data and Network Science, 7(2), 667-676.

Shwedeh, F., Aburayya, A., Alfaisal, R., Adelaja, A. A., Ogbolu, G., Aldhuhoori, A., & Salloum, S. A. (2022b). SMEs' Innovativeness and Technology Adoption as Downsizing Strategies during COVID-19: The Moderating Role of Financial Sustainability in the Tourism Industry Using Structural Equation Modelling. Sustainability, 14(23), 16044. https://doi.org/10.3390/su142316044

El Nokiti, A., Shaalan, K., Salloum, S., Aburayya, A., Shwedeh, F., Shameem , B. (2022). Is Blockchain the answer? A qualitative Study on how Blockchain Technology Could be used in the Education Sector to Improve the Quality of Education Services and the Overall Student Experience. Computer Integrated Manufacturing Systems, 28 (11), 543-556.

Shwedeh, F., Hami, N., Abu Bakar, S. (2021). Dubai smart city and residence happiness: A conceptual study. Annals of the Romanian Society for Cell Biology, 25, Issue 1, 2021, Pages. 7214 – 7222.

Shwedeh, F., Adelaja, A. A., Ogbolu, G., Kitana, A., Taamneh, A., Aburayya, A., & Salloum, S. A. (2023). Entrepreneurial innovation among international students in the UAE: Differential role of entrepreneurial education using SEM analysis. International Journal of Innovative Research and Scientific Studies, 6(2), 266-280.

Ravikumar, A., Kitana, A., Taamneh, A., Aburayya, A., Shwedeh, F., Salloum, S., Shaalan.,K. (2022). Impact of knowledge sharing on knowledge Acquisition among Higher Education Employees. Computer Integrated Manufacturing Systems, 28 (12), 827-845.

Ravikumar, R., Kitana, A., Taamneh, A., Aburayya, A., Shwedeh, F., Salloum, S., & Shaalan, K. (2023). The Impact of Big Data Quality Analytics on Knowledge Management in Healthcare Institutions: Lessons Learned from Big Data's Application within The Healthcare Sector. South Eastern European Journal of Public Health. Retrieved from http://seejph.com/index.php/seejph/article/view/309

Salameh, M., Taamneh, A., Kitana, A., Aburayya, A., Shwedeh, F., Salloum, S., ... & Varshney, D. (2022). The Impact of Project Management Office's Role on Knowledge Management: A Systematic Review Study. Computer Integrated Manufacturing Systems, 28(12), 846-863.

Abdallah, S., Al Azzam, B., El Nokiti, A.Salloum, S., Aljasmi, S., Aburayya, A., Shwedeh, F. (2022). A COVID19 Quality Prediction Model based on IBM Watson Machine Learning and Artificial Intelligence Experiment. Computer Integrated Manufacturing Systems, 28(11), 499-518.

Dahu, B. M., Aburayya, A., Shameem., B., Shwedeh, F., Alawadhi, M., Aljasmi , S., Salloum, S. A. (2023). The Impact of COVID-19 Lockdowns on Air Quality: A Systematic Review Study. South Eastern European Journal of Public Health. Retrieved from http://www.seejph.com/index.php/seejph/article/view/312

Alkashami, M., Taamneh, A., Khadragy, S., Shwedeh, F., Aburayya, A & Salloum, S. (2023). AI different approaches and ANFIS data mining: A novel approach to predicting early employment readiness in middle eastern nations. International Journal of Data and Network Science, 7(3), 1267-1282.

Khadragy, S., Elshaeer, M., Mouzaek, T., Shammass, D., Shwedeh, F., Aburayya, A., ... & Aljasmi, S. (2022). Predicting Diabetes in United Arab Emirates Healthcare: Artificial Intelligence and Data Mining Case Study. South Eastern European Journal of Public Health.

Shwedeh, F., Hami, N., & Baker, S. Z. A. (2020). Effect of leadership style on policy timeliness and performance of smart city in Dubai: a review. In Proceedings of the International Conference on Industrial Engineering and Operations Management (pp. 917-922).

Shwedeh, F. (2024). Harnessing digital issue in adopting metaverse technology in higher education institutions: Evidence from the United Arab Emirates. International Journal of Data and Network Science, 8(1), 489-504.