The Intersection of Public Health and Cyber Security: Lessons from the COVID-19 Pandemic

Kassym-Jomart Carlos Alberto Hernández
Universidad Autónoma de Nayarit
Ciudad de la Cultura Amado Nervo, Boulevard Enrique Díaz de León S/N, Cd. de la Cultura, 63190 Tepic, Nay., Mexico

Abstract

The COVID-19 pandemic has brought to the forefront the critical intersection of public health and cybersecurity. As health systems worldwide grappled with unprecedented challenges, the pandemic simultaneously exposed the vulnerabilities of health information systems to cyber threats. This research provides an in-depth exploration of the lessons learned from the COVID-19 pandemic regarding the intersection of public health and cybersecurity. The paper begins by providing an overview of the roles of public health and cybersecurity, highlighting their interconnectedness. It then delves into the pre-pandemic role of cybersecurity in public health, emphasizing the importance of data protection in health systems. The paper further explores the impact of the COVID-19 pandemic on both public health and cybersecurity, illustrating the surge in cyber threats during this period and the corresponding effects on public health data and systems. Drawing from various case studies, the paper elucidates the lessons learned from the pandemic in terms of public health data protection and cybersecurity response. It underscores the gaps and challenges exposed by the pandemic and how they were addressed, providing a comprehensive analysis of the cybersecurity landscape during this global health crisis. The paper provides recommendations for strengthening cybersecurity measures in public health, emphasizing the need for robust data protection strategies, increased cybersecurity awareness, and the integration of cybersecurity in public health policies and practices. Through this research, the paper underscores the urgent need for robust cybersecurity measures in public health. It highlights the importance of safeguarding sensitive health data and ensuring the resilience of health systems in the face of future pandemics. The findings of this research contribute to the ongoing discourse on the intersection of public health and cybersecurity, providing valuable insights for policymakers, health professionals, and cybersecurity experts.

Keywords: *Health Information Technology, Healthcare Reform, Opportunities, Challenges, Patient Outcomes*

Introduction

The 21st century has been characterized by the rapid digitalization of various sectors, including public health [1]–[3]. The integration of technology into public health has revolutionized healthcare delivery, disease surveillance, and health research, leading to improved health outcomes and efficiency. However, this digital transformation has also introduced a new set of challenges, particularly in the realm of cybersecurity. The protection of sensitive health data has become a paramount concern in the digital age, given the potential consequences of data breaches [4], [5]. These consequences range

from identity theft and financial fraud to threats to public health and safety. The COVID-19 pandemic, which swept across the globe in 2020, has further underscored the critical intersection of public health and cybersecurity, revealing vulnerabilities in health information systems and the dire consequences of their exploitation.

The disease primarily affects the respiratory system, but its influence extends to multiple organ systems, including the cardiovascular system. Symptoms associated with the virus range from mild to severe, with severe cases often resulting in pneumonia, Acute Respiratory Distress Syndrome (ARDS), and other life-threatening complications. There are also potential long-term consequences for some patients, which are collectively referred to as Long-COVID or Post-Acute Sequelae of SARS-CoV-2 infection (PASC). POTS is a condition characterized by an abnormal increase in heart rate that occurs upon standing up and can cause symptoms such as lightheadedness, fainting, and rapid heartbeat. In the context of COVID-19, it has been proposed that the virus may trigger POTS in some individuals through mechanisms such as direct viral damage or post-viral autoimmunity [6]. It is also been observed that COVID-19 can have diverse effects on the cardiovascular system [7], [8]. In some cases, the virus may lead to direct myocardial injury, acute myocarditis, and myocardial infarction due to a pro-thrombotic state. Moreover, there's evidence suggesting that pre-existing cardiovascular disease is associated with worse outcomes in patients with COVID-19 [9]. More research is necessary to further elucidate these associations and potential underlying mechanisms.

Declared a Public Health Emergency of International Concern by the World Health Organization in January 2020, the COVID-19 pandemic has had far-reaching impacts on global health systems [10]. The pandemic has strained healthcare resources, disrupted routine health services, and posed significant challenges to disease surveillance and control. As countries grappled with the health crisis, the pandemic also exposed the vulnerabilities of health information systems to cyber threats. Cybercriminals exploited the crisis, launching a wave of cyberattacks targeting healthcare institutions, research organizations, and public health agencies [11], [12]. These attacks not only threatened the integrity of health data but also disrupted healthcare services, thereby exacerbating the public health crisis.

This research paper aims to delve into the lessons learned from the COVID-19 pandemic regarding the intersection of public health and cybersecurity. It seeks to understand the role of cybersecurity in public health before the pandemic, the impact of COVID-19 on both domains, and the lessons learned from this global health crisis. The paper further discusses future implications and provides recommendations for strengthening cybersecurity in public health. The findings of this research are expected to contribute to the ongoing discourse on the intersection of public health and cybersecurity, providing valuable insights for policymakers, health professionals, and cybersecurity experts [13], [14].

The paper begins by providing an overview of the roles of public health and cybersecurity, highlighting their interconnectedness. It then explores the pre-pandemic

role of cybersecurity in public health, emphasizing the importance of data protection in health systems. The paper further discusses the impact of the COVID-19 pandemic on both public health and cybersecurity, illustrating the surge in cyber threats during this period and the corresponding effects on public health data and systems. Drawing from various case studies, the paper elucidates the lessons learned from the pandemic in terms of public health data protection and cybersecurity response. It concludes by discussing the future implications of these lessons for public health and cybersecurity and provides recommendations for strengthening cybersecurity measures in public health. Through this research, the paper underscores the urgent need for robust cybersecurity measures in public health. It highlights the importance of safeguarding sensitive health data and ensuring the resilience of health systems in the face of future pandemics. The findings of this research contribute to the ongoing discourse on the intersection of public health and cybersecurity, providing valuable insights for policymakers, health professionals, and cybersecurity experts.

Data in Public Health

Data plays a pivotal role in public health. It is the cornerstone of public health research, policy-making, and practice. Public health data, which includes information about disease prevalence, health behaviors, environmental exposures, and social determinants of health, is essential for identifying health trends, monitoring disease outbreaks, and evaluating the effectiveness of health interventions. It informs the development of public health policies and programs, guiding resource allocation and decision-making. Furthermore, data is crucial for health communication, providing the evidence needed to raise awareness about health issues and advocate for health-promoting policies [15].

The importance of data in public health underscores the need for robust cybersecurity measures. Cybersecurity, which involves protecting information systems from theft or damage, plays a critical role in safeguarding health data [16]. As health systems increasingly rely on digital technologies, the volume of health data has grown exponentially, making it a prime target for cybercriminals. Cybersecurity measures, including data encryption, secure user authentication, and intrusion detection systems, are necessary to protect the confidentiality, integrity, and availability of health data [17]. These measures not only prevent unauthorized access to health data but also ensure that health information systems remain functional and reliable, thereby supporting the continuity of health services [18].

Even before the COVID-19 pandemic, there were several instances where cybersecurity incidents had a significant impact on public health. For example, in 2017, the WannaCry ransomware attack affected numerous organizations worldwide, including the National Health Service (NHS) in the UK. The attack led to the cancellation of around 19,000 appointments, costing the NHS an estimated £92 million. Another example is the 2015 attack on the health insurance company Anthem, where hackers stole the personal information of nearly 78.8 million individuals, including their names, birthdays, medical IDs, social security numbers, street addresses, email addresses, and employment information. These incidents underscore the potential consequences of

cybersecurity breaches on public health, highlighting the need for robust cybersecurity measures in health systems.

The COVID-19 pandemic has had a profound impact on both public health and cybersecurity. On the public health front, the pandemic has strained health systems, disrupted routine health services, and posed significant challenges to disease surveillance and control. On the cybersecurity front, the pandemic has led to a surge in cyber threats. As health systems rapidly digitalized their operations in response to the pandemic, cybercriminals exploited the crisis to launch a wave of cyberattacks targeting healthcare institutions, research organizations, and public health agencies [19], [20]. These attacks have threatened the integrity of health data and disrupted healthcare services, exacerbating the public health crisis. The pandemic has underscored the critical intersection of public health and cybersecurity, highlighting the urgent need for robust cybersecurity measures in health systems [21].

Challenges COVID-19 and global public health

The COVID-19 pandemic has had a profound impact on public health globally. It has not only caused a significant number of illnesses and deaths but has also strained health systems, disrupted routine health services, and exacerbated existing health disparities. The pandemic has affected every aspect of public health, from disease surveillance and control to health communication and policy-making.

The pandemic has strained health systems worldwide. Hospitals and healthcare facilities have been overwhelmed with COVID-19 patients, leading to shortages of beds, ventilators, and other critical resources. Healthcare workers have faced immense pressure, working long hours in high-risk environments. The pandemic has also disrupted routine health services, including immunization, maternal and child health services, and non-communicable disease management. These disruptions have had significant health consequences, leading to increases in mortality and morbidity from conditions other than COVID-19.

The pandemic has also exacerbated existing health disparities. Vulnerable populations, including the elderly, people with underlying health conditions, racial and ethnic minorities, and low-income individuals, have been disproportionately affected by the pandemic. These populations have higher rates of COVID-19 infection and mortality and have faced greater barriers to accessing healthcare services during the pandemic.

The COVID-19 pandemic has also led to a surge in cyber threats. As health systems rapidly digitalized their operations in response to the pandemic, cybercriminals exploited the crisis to launch a wave of cyberattacks. These attacks have targeted healthcare institutions, research organizations, and public health agencies, threatening the integrity of health data and disrupting healthcare services.

Cyber threats during the pandemic have taken various forms, including phishing attacks, ransomware attacks, and data breaches [22]. Phishing attacks have exploited the fear and uncertainty surrounding the pandemic to trick individuals into revealing sensitive information or downloading malicious software. Ransomware attacks have

targeted healthcare institutions, encrypting their data and demanding ransom for its release [23]. Data breaches have involved the unauthorized access to or disclosure of sensitive health data.

Several cybersecurity incidents during the COVID-19 pandemic highlight the scale and severity of these threats. For instance, in March 2020, the University Hospital Brno in the Czech Republic, a major COVID-19 testing hub, had to shut down its entire IT network due to a ransomware attack. This incident disrupted the hospital's operations, delaying surgical procedures and compromising the hospital's ability to provide critical care. In another instance, the U.S. Health and Human Services Department suffered a cyberattack in March 2020 aimed at slowing the agency's response to the COVID-19 pandemic. Although the attack did not result in a significant data breach, it underscored the vulnerability of health institutions to cyber threats during the pandemic [24].

The COVID-19 pandemic has provided several important lessons regarding the intersection of public health and cybersecurity. First, it has underscored the critical importance of cybersecurity in health system [25], [26]s. The surge in cyber threats during the pandemic has highlighted the need for robust cybersecurity measures to protect sensitive health data and ensure the continuity of health services [27]. Second, the pandemic has highlighted the need for greater cybersecurity awareness among healthcare professionals. Many cyber threats exploit human vulnerabilities, such as the tendency to click on suspicious links or download malicious software. Therefore, training healthcare professionals in cybersecurity best practices is crucial to preventing cyber threats. Third, the pandemic has underscored the need for collaboration in addressing cyber threats [28]. This includes collaboration between different sectors, such as healthcare and IT, and between different entities, such as public health agencies, healthcare institutions, and cybersecurity firms. Such collaboration can facilitate the sharing of threat intelligence, the development of cybersecurity standards and guidelines, and the coordination of response efforts to cyber threats.

Response to Cybersecurity Threats During the Pandemic

The response to cybersecurity threats during the COVID-19 pandemic has been multifaceted, involving various stakeholders, including governments, healthcare institutions, cybersecurity firms, and international organizations. Governments have played a crucial role in coordinating the response to cyber threats, issuing warnings about potential threats, and providing guidance to healthcare institutions on how to protect their information systems. Cybersecurity firms have worked closely with healthcare institutions to detect and respond to cyber threats, offering their services pro bono in some cases. International organizations, such as the World Health Organization and Interpol, have also played a key role in facilitating international cooperation in response to cyber threats.

Despite these efforts, the response to cybersecurity threats during the pandemic has faced several challenges. These include the rapid digitalization of health services, which has expanded the attack surface for cybercriminals; the lack of cybersecurity awareness among healthcare professionals, which has made health systems more vulnerable to

threats; and the limited resources available for cybersecurity in many healthcare institutions, particularly in low- and middle-income countries. The COVID-19 pandemic has provided several important lessons in terms of public health data protection. First, it has underscored the critical importance of data protection in health systems. The surge in cyber threats during the pandemic has highlighted the need for robust data protection measures to safeguard sensitive health data.

Second, the pandemic has highlighted the need for data protection to be integrated into all aspects of health systems, from clinical care to research. This includes implementing technical measures, such as data encryption and secure user authentication, as well as administrative measures, such as data protection policies and training programs [29]. Third, the pandemic has underscored the need for a risk-based approach to data protection. This involves identifying potential risks to health data, assessing their likelihood and potential impact, and implementing measures to mitigate these risks [30], [31].

Based on the lessons learned from the pandemic, several suggestions can be made for improving cybersecurity in public health. First, there is a need for greater investment in cybersecurity in health systems. This includes investing in cybersecurity infrastructure, such as firewalls and intrusion detection systems, as well as in cybersecurity personnel and training programs [32]. Second, there is a need for greater collaboration in addressing cyber threats. This includes collaboration between different sectors, such as healthcare and IT, and between different entities, such as public health agencies, healthcare institutions, and cybersecurity firms [33]. Third, there is a need for stronger regulations and standards for data protection in health systems. This includes developing and enforcing data protection laws and regulations, as well as adopting international standards for data protection in healthcare [34].

The COVID-19 pandemic has underscored the critical intersection of public health and cybersecurity, highlighting the urgent need for robust cybersecurity measures in health systems. Looking forward, it is crucial that the lessons learned from the pandemic inform efforts to strengthen cybersecurity in public health. First, there is a need for greater investment in cybersecurity in health systems. This includes investing in cybersecurity infrastructure, personnel, and training programs. Governments, donors, and healthcare institutions should prioritize cybersecurity in their budgets and strategic plans. Second, there is a need for stronger regulations and standards for data protection in health systems. Governments should develop and enforce robust data protection laws and regulations. Healthcare institutions should adopt international standards for data protection and should be held accountable for breaches of these standards. Third, there is a need for greater collaboration in addressing cyber threats. This includes fostering collaboration between different sectors and entities, facilitating the sharing of threat intelligence, and coordinating response efforts to cyber threats.

Conclusion

The COVID-19 pandemic has underscored the critical intersection of public health and cybersecurity, highlighting the urgent need for robust cybersecurity measures in health

systems. As we move into the post-COVID-19 era, cybersecurity will continue to play a crucial role in public health.

Firstly, the digitalization of health services, which was accelerated by the pandemic, is likely to continue in the post-COVID-19 era. This includes the use of telemedicine, electronic health records, and digital health technologies, such as mobile health apps and wearable devices. As health systems become increasingly digital, the need for cybersecurity will become even more critical.

Secondly, the threat landscape is likely to evolve in the post-COVID-19 era. Cybercriminals are becoming increasingly sophisticated, employing advanced techniques to breach health information systems. Furthermore, the increasing value of health data, particularly genetic and biometric data, is likely to make health systems a prime target for cyberattacks.

Thirdly, the integration of cybersecurity into public health policy and practice is likely to become a key focus in the post-COVID-19 era. This includes the development of public health policies and guidelines on cybersecurity, the integration of cybersecurity into public health education and training, and the inclusion of cybersecurity in public health research. In light of the lessons learned from the COVID-19 pandemic and the anticipated future trends, it is crucial to strengthen cybersecurity in public health. Several recommendations can be proposed to achieve this goal. Firstly, there is a pressing need to invest in cybersecurity infrastructure and personnel [35]. Governments, donors, and healthcare institutions should prioritize this investment. This involves allocating resources to secure hardware and software, recruiting skilled cybersecurity professionals, and providing ongoing cybersecurity training for all staff members. These measures will help to fortify the defenses against cyber threats and ensure the integrity and security of health data.

Secondly, the development and enforcement of robust data protection regulations are paramount. Governments should take the lead in establishing and enforcing stringent data protection laws and regulations. These regulations should aim to protect the privacy and security of health data, hold healthcare institutions accountable for data breaches, and provide remedies for individuals whose data has been compromised. This legal framework will serve as a deterrent to potential cyber threats and provide a sense of security to individuals whose data is held by healthcare institutions.

Thirdly, fostering collaboration in addressing cyber threats is essential. This involves encouraging greater cooperation between different sectors and entities, such as the healthcare and IT sectors. Facilitating the sharing of threat intelligence and coordinating response efforts to cyber threats are also crucial elements of this collaborative approach. By working together, these sectors can pool their resources and expertise to combat cyber threats more effectively.

Fourthly, the integration of cybersecurity into public health policy and practice is necessary. This involves developing public health policies and guidelines that incorporate cybersecurity considerations, integrating cybersecurity into public health

education and training, and including cybersecurity in public health research. By embedding cybersecurity into the fabric of public health, we can ensure that it is not an afterthought but a key consideration in all public health initiatives.

Lastly, promoting cybersecurity awareness is crucial. There is a need for greater cybersecurity awareness among healthcare professionals and the general public. This involves providing education and training on cybersecurity best practices, raising awareness about the risks of cyber threats, and promoting responsible behavior online. By increasing cybersecurity awareness, we can empower individuals to protect themselves and their data from cyber threats.

References

[1] S. Bhaskar, A. Nurtazina, S. Mittoo, M. Banach, and R. Weissert, "Editorial: Telemedicine During and Beyond COVID-19," *Frontiers in Public Health*, vol. 9, 2021.

[2] F. Antunes, R. Cordeiro, and A. Virgolino, "Monkeypox: From A Neglected Tropical Disease to a Public Health Threat," *Infect. Dis. Rep.*, vol. 14, no. 5, pp. 772–783, Sep. 2022.

[3] Y. Zhu, Y. Sha, H. Wu, M. Li, R. A. Hoffman, and M. D. Wang, "Proposing Causal Sequence of Death by Neural Machine Translation in Public Health Informatics," *IEEE J Biomed Health Inform*, vol. 26, no. 4, pp. 1422–1431, Apr. 2022.

[4] S. E. Jasper, "US cyber threat intelligence sharing frameworks," *Int. J. Intell. CounterIntelligence*, 2017.

[5] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, and B.-T. Chu, "Data-driven analytics for cyber-threat intelligence and information sharing," *Comput. Secur.*, vol. 67, pp. 35–58, Jun. 2017.

[6] D. Mallick, L. Goyal, P. Chourasia, M. R. Zapata, K. Yashi, and S. Surani, "COVID-19 Induced Postural Orthostatic Tachycardia Syndrome (POTS): A Review," *Cureus*, vol. 15, no. 3, p. e36955, Mar. 2023.

[7] R. A. Ocher, E. Padilla, J. C. Hsu, and P. R. Taub, "Clinical and Laboratory Improvement in Hyperadrenergic Postural Orthostatic Tachycardia Syndrome (POTS) after COVID-19 Infection," *Case Rep Cardiol*, vol. 2021, p. 7809231, Aug. 2021.

[8] S. Reddy, S. Reddy, and M. Arora, "A Case of Postural Orthostatic Tachycardia Syndrome Secondary to the Messenger RNA COVID-19 Vaccine," *Cureus*, vol. 13, no. 5, p. e14837, May 2021.

[9] M. Abdelghany *et al.*, "CRT-200.08 outcomes of acute coronary syndrome in patients with Coronavirus 2019 infection: A systematic review and meta-analysis," *Cardiovascular Interventions*, vol. 15, no. 4_Supplement, pp. S29–S30, Feb. 2022.

[10] A. Bodepudi and M. Reddy, "The Rise of Virtual Employee Monitoring in Cloud and Its Impact on Hybrid Work Choice," *Journal of Artificial Intelligence and Machine Learning in Management*, vol. 5, no. 1, pp. 25–50, 2021.

[11] I. Sarhan and M. Spruit, "Open-CyKG: An Open Cyber Threat Intelligence Knowledge Graph," *Knowledge-Based Systems*, vol. 233, p. 107524, Dec. 2021.

[12] R. Brown and R. M. Lee, "The evolution of cyber threat intelligence (cti): 2019 sans cti survey," *SANS Institute. Available online: https://www. sans. org/white-papers/38790/(accessed on 12 July 2021)*, 2019.

[13] K. A. Abdullah and W. Reed, "3D printing in medical imaging and healthcare services," *J Med Radiat Sci*, vol. 65, no. 3, pp. 237–239, Sep. 2018.
[14] A. Kichloo *et al.*, "Telemedicine, the current COVID-19 pandemic and the future: a narrative review and perspectives moving forward in the USA," *Fam Med Community Health*, vol. 8, no. 3, Aug. 2020.
[15] A. Bodepudi and M. Reddy, "Cloud-Based Biometric Authentication Techniques for Secure Financial Transactions: A Review," *IJIC*, vol. 4, no. 1, pp. 1–18, Jan. 2020.
[16] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, Scottsdale, Arizona, USA, 2014, pp. 51–60.
[17] K. Nova, "Analyzing Keystroke Dynamics for User Authentication: A Comparative Study of Feature Extractions and Machine Learning Models," *Sage Science Review of Applied Machine Learning*, vol. 5, no. 2, pp. 67–80, 2022.
[18] M. Reddy and A. Bodepudi, "Analysis of Cloud Based Keystroke Dynamics for Behavioral Biometrics Using Multiclass Machine Learning," *RRST*, vol. 2, no. 1, pp. 120–135, Oct. 2022.
[19] J. W. Luk, S. E. Gilman, K. R. Sita, C. Cheng, D. L. Haynie, and B. G. Simons-Morton, "Cyber behaviors among heterosexual and sexual minority youth: Subgroup differences and associations with health indicators," *Cyberpsychol. Behav. Soc. Netw.*, vol. 22, no. 5, pp. 315–324, May 2019.
[20] S. S. Gopalan, A. Raza, and W. Almobaideen, "IoT Security in Healthcare using AI: A Survey," in *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2021, pp. 1–6.
[21] A. Bodepudi and M. Reddy, "Cloud-Based Gait Biometric Identification in Smart Home Ecosystem," *International Journal of Intelligent Automation and Computing*, vol. 4, no. 1, pp. 49–59, 2021.
[22] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. London, England: Auerbach, 2016.
[23] K. Nova, A, Umaamaheshvari, S. S. Jacob, G. Banu, M. S. P. Balaji, and S, Srithar, "Floyd–Warshalls algorithm and modified advanced encryption standard for secured communication in VANET," *Measurement: Sensors*, vol. 27, p. 100796, Jun. 2023.
[24] K. Nova, "Machine Learning Approaches for Automated Mental Disorder Classification based on Social Media Textual Data," *CIBSS*, vol. 7, no. 1, pp. 70–83, Apr. 2023.
[25] N. S. Alan, A. K. Karagozoglu, and T. Zhou, "Firm-level cybersecurity risk and idiosyncratic volatility," *J. Portf. Manag.*, vol. 47, no. 9, pp. 110–140, Sep. 2021.
[26] G. Gomez, E. Espina, J. Armas-Aguirre, and J. M. M. Molina, "Cybersecurity architecture functional model for cyber risk reduction in IoT based wearable devices," in *2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)*, Bogotá, Colombia, 2021.
[27] A. Bodepudi and M. Reddy, "Spoofing Attacks and Mitigation Strategies in Biometrics-as-a-Service Systems," *ERST*, vol. 4, no. 1, pp. 1–14, Feb. 2020.
[28] S. Samtani, M. Abate, V. Benjamin, and W. Li, "Cybersecurity as an industry: A cyber threat intelligence perspective," *The Palgrave Handbook of*, 2020.

[29] K. Nova, "AI-Enabled Water Management Systems: An Analysis of System Components and Interdependencies for Water Conservation," *ERST*, vol. 7, no. 1, pp. 105–124, Jun. 2023.
[30] P. Kalogeropoulos, D. Papanikas, and P. Kotzanikolaou, "A distributed model for privacy preserving V2I communication with strong unframeability and efficient revocation," *J. Cybersecur. Priv.*, vol. 2, no. 4, pp. 778–799, Sep. 2022.
[31] A. J. Taylor, "Recognizing cybersecurity threats in healthcare settings for effective risk management," in *Mobile Medicine*, New York: Productivity Press, 2021, pp. 177–182.
[32] K. Nova, "Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence," *International Journal of Information and Cybersecurity*, vol. 6, no. 1, pp. 21–42, 2022.
[33] K. Kucia, "Enterprise cybersecurity risk management in the era of the covid-19 epidemic threat," *Zesz. Nauk. Wyższej Szk. Humanit. Zarz.*, vol. 22, no. 3, pp. 133–141, Sep. 2021.
[34] P. A. Wortman and J. A. Chandy, "SMART: security model adversarial risk-based tool for systems security design evaluation," *J. Cybersecur.*, vol. 6, no. 1, Jan. 2020.
[35] G. Varma, R. Chauhan, and D. Singh, "Sarve: synthetic data and local differential privacy for private frequency estimation," *Cybersecurity*, vol. 5, no. 1, p. 26, Aug. 2022.