Journal of Scientific and Technical Research
13 (2) 2023, 24-31
http://www.publishingindia.com/jstr

Protect Imminent Cyber Threats in Digital Security – Post-COVID'19

Kuldeep Chouhan[1*], Jyoti Prakash Bora[2], Prateek Kumar Gupta[2] and Mohammad Danish[2]
[1]Professor, Department of Computer Science and Applications, School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India
[2]Under Graduate Student, Department of Computer Science and Applications, School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India
[*]Corresponding Author: kuldeep.chouhan@sharda.ac.in

Abstract: In this study, digital security focuses on imminent cybersecurity for remote workstations and protection from future threats. This work proposes how digital security broadens cybersecurity energies that provide an outlook of cybersecurity in the light of targets, threats, and preventive measures. Remote work cybersecurity research emphasizes risks associated with personal devices and home networks. Post-COVID'19, cybersecurity requires training, virtual private networks (VPNs), and encryption that makes a robust security around the users. Collaboration tools require improved security, and human factors like phishing are crucial. The threat of ransomware to remote workers is increasing. The emphasis is on a thorough approach to protect remote work from changing risks. For instance, machine learning improves intrusion detection by learning from prior attacks, while artificial intelligence (AI) able to identify unusual online banking activity and enhances digital security by automating processes, speeding up responses, and adjusting to changing threats. Furthermore, a global parallel is a proactive manner in healthy cybersecurity, accentuating the worldwide prerequisite to strengthening digital security in a post-COVID-19 world of digital energy.

Keywords: COVID'19 epidemic, Cybercrime, Cybersecurity, Cyberthreats, Simulations in cybersecurity.

I. Introduction

Effects of the Novel Coronavirus known as COVID'19 and SARS-CoV-2, has reverberated across the globe. With over 12.5 million confirmed infections reported worldwide [1]. Unfortunately, an estimated 400,000 patients out of a sample of about 6 million have succumbed to the virus's effects [1], and numbers continue to rise as the pandemic persists. Recent data from the World Health Organization (WHO) underscores the ongoing severity of the situation with over 4.5 million new cases and more than 76,000 new deaths reported in a single week in April 2021, reflecting a persistent upward trend [2].

Governments around the world, including India, have implemented a series of far-reaching measures to curb the spread of the virus, including lockdowns, quarantines, remote work, virtual education, and travel restrictions [2]. Consequently, various nations have increasingly turned to personal electronic devices to carry out professional, academic, and personal tasks [3, 4, 5, 6, 7]. The virtualization of daily activities, driven by the necessity of social distancing and remote engagement, has led to an unprecedented shift in routines, creating both opportunities and vulnerabilities.

The emergence of a virtualized existence has innovative avenues for cybercriminals [8] [9]. The uncertainty halting from disrupted routines provides abundant ground for cyberattacks, and extended dependence on digital platforms creates an array of potential attack vectors. Federal Bureau of Investigation (FBI) indicates a staggering 400% increase in cybercrime during the pandemic [3]. Correspondingly, it has reported a rise in cybercrimes during the COVID-19 crisis [4], prominence the urgency of addressing the evolving landscape of cybersecurity threats amidst the global health emergency. As India, along with the rest of the world, contends with the ongoing challenges of the pandemic, understanding and mitigating the escalating risks posed by cybercriminals are crucial components of safeguarding both digital and physical well-being. This study investigates the intricate interplay between the pandemic and the surge in cyber threats, shedding light on the heightened vulnerabilities and the urgent need for effective countermeasures.

This demonstrates the value of user education and training to raise their awareness of cybersecurity. Thus, the investigation of the various cyberthreat vectors connected to the pandemic and the exploration of potential preventive measures are the main goals of this work. This work discusses the distribution of the attacks and makes an effort to comprehend the objectives and attack surfaces of the attackers when studying cyberattacks connected to COVID-19. This supports the creation of mitigation measures and includes a description of the topics covered in a nutshell as shown in Fig. 1.

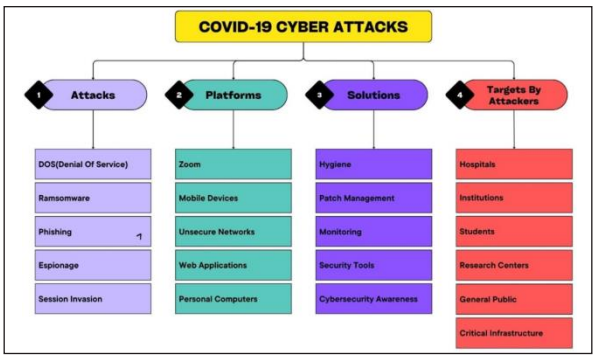

Fig. 1: Attacks and Solutions in Cybersecurity

A. Benefits of Digital Changes

Among the challenges posed by the COVID-19 pandemic and the subsequent surge in cyber threats, certain unexpected benefits have emerged. The accelerated adoption of digital platforms in India and beyond has facilitated rapid communication, enabled remote collaboration, and sustained essential services even in the face of stringent lockdowns and physical distancing measures. Furthermore, the heightened reliance on technology has propelled innovations in various sectors, driving the evolution of digital healthcare, e-commerce, and online education. As society navigates the complexities of this new reality, it is imperative to acknowledge and harness these positive outcomes, while remaining vigilant about the potential risks that accompany the digital transformation.

B. Applications of Digital Security

The impact of the COVID-19 pandemic and the subsequent shift towards digitalization has been particularly evident in the diverse range of applications that have emerged around the world.

- From contact tracing and remote patient monitoring in healthcare to virtual conferences and online marketplaces, technology has played a pivotal role in ensuring continuity across various sectors.
- Educational institutions have swiftly transitioned to digital learning platforms, enabling students to access educational resources from the safety of their homes.
- Various businesses have adapted by embracing e-commerce and remote work arrangements, redefining the traditional boundaries of operations.
- Innovative applications not only underscore the adaptability of society but also highlight the potential for technology to reshape the way of live, work, and interact, creating new opportunities for growth and development in the digital age.

C. Digital Security in Post-Pandemic

The rapid digital transformation triggered by the COVID-19 pandemic has unveiled both the advantages and vulnerabilities of an increasingly interconnected world. As we reflect on the experiences of this pandemic and consider the potential for future health crises, the impacts of digital security on society become all the more apparent. The lessons learned from navigating cyber threats and safeguarding critical data during the pandemic will inevitably shape our approach to future health emergencies. This includes fortifying digital infrastructure to mitigate the risk of cyberattacks on essential services, enhancing data privacy measures, and fostering international collaboration to combat emerging cyber threats.

II. Literature Survey

The COVID-19 pandemic has changed the world's landscape, forcing people and organizations to rely more and more on information and communication technologies (ICTs) to adjust to the new conditions. Digital connections became the support for organizations, industries, and healthcare providers as the world struggled with unprecedented health crises, enabling remote work, telemedicine, and data sharing. The need for reliable digital infrastructure has increased but quick digital change has resulted in an alarming rise in cyberattacks. While the COVID-19 pandemic has helped in the fight against the virus's propagation, also exacerbated the worrisome rise in cybercrime. The emphasis must turn to strengthening cybersecurity measures to protect user data and reduce evolving cyber risks to prevent a potential sequel crisis.

This study takes on the vital duty of determining how the COVID-19 pandemic has affected cybersecurity, providing a thorough evaluation of all affected areas. The research employs a systematic review of the literature that covers the period of December 2019 to June 2020 and includes international research papers on cybersecurity challenges brought on by the pandemic. The statistics highlight an exponential rise in cyberattacks and threats as the epidemic consumed the world economy. During this time, large enterprises, medical facilities, and governmental organizations found themselves the target of cybercriminals, adding to the difficulties already faced by the novel coronavirus. Consequently, the study emphasizes the need to address the parallel danger of cybercrimes alongside the pandemic and encourages individuals and organizations to implement proactive cybersecurity actions to preserve their data and information systems infrastructure.

An interaction between the COVID-19 pandemic and cybersecurity forced people to adopt digital solutions for basic needs and also revealed weaknesses in our digital ecosystem. By categorizing and comprehending cyber occurrences related to COVID-19, our research contributes significant

new insights into the dynamic threat landscape. Additionally, it clarifies the international reaction to the epidemic and highlights the value of appropriate information exchange to lessen its effects. The work explores difficulties particular to the area and provides practical mitigation techniques in the Indian context, where cybersecurity readiness is of the utmost importance. Particularly, COVID-19 has emphasized the need for an essential change in how cybersecurity is treated, emphasizing the significance of creating trust, new technological interactions, and personal support as the most important cybersecurity assets. It becomes clear that maintaining our privacy and protecting our physical health are now inextricably linked, making cybersecurity a crucial element of the post-pandemic society.

III. Overview of Cybersecurity

The COVID-19 disruption has highlighted the institutions' shortcomings in defending the health and welfare of people. rising harms have resulted from a lack of timely and accurate data as well as pervasive misinformation, and there is a rising conflict between data privacy and public health issues. The COVID-19-related suffering has gotten worse due to the lack of good statistics and trustworthy information. The COVID-19 dilemma is both a trust and an information crisis. It has highlighted the trust and data-sharing shortcomings of the current systems. Main supply chain breakdowns have been observed during the crisis, particularly for personal protective equipment (PPE) and life-supporting ventilators in clinics and hospitals [16].

The COVID-19 pandemic has seen significant use of digital approaches. However, there are issues with telemedicine and other digital technologies for protecting information privacy and security [17]. The number of cyberattacks has significantly increased since the start of the COVID-19 epidemic. Major cyber dangers during the pandemic are brought on by both human error, system and technological breakdowns. Operational risk comes from human behaviour, including deliberate (such as theft, fraud, and vandalism), unintentional (such as omissions, errors, and blunders), and passive (such as lack of availability, knowledge, skills, and direction). Software (i.e., coding standards, testing, security settings, change control, configuration management, and compatibility), hardware (i.e., capacity, performance, maintenance, and obsolescence), and system failures account for the majority of technological system and technology failures [18].

A. Effects of COVID-19 in Society

The Chinese province of Hubei, reported an outbreak of a novel coronavirus-related viral illness in December 2019, Wuhan [19]. The novel COVID-19 is a member of the same coronavirus as the Middle East Respiratory Syndrome (MERS) [20] which is the source of two outbreaks, and the acute respiratory syndrome (SARS) [21]. All age groups are affected by the new virus, which primarily spreads by respiratory droplets and direct contact [22]. The World Health Organisation (WHO) proclaimed an epidemic in December 2021 as a result of the disease's high mortality rates, rapid virus propagation, and rise in infections [23]. The WHO estimates that as of December 6, 2021, the virus had killed 530,5337 individuals worldwide and infected 269,559,230 others. As of December 6, 2021, this virus had also infected 6,137,821 people in Iran and claimed the lives of 130,277 people [24,25].

B. Significant Effects in Digital Security Post-Pandemic in Rural Areas

In rural areas, major repercussions from the COVID-19 pandemic in both short-term and long-term. Following are a few of the major impacts of COVID-19 on Indian rural areas includes;

i. Healthcare Challenges

In India, access to healthcare services in rural regions has long been a problem. The pandemic made these issues worse. Numerous towns lacked a strong healthcare system, which made it challenging to diagnose, treat, and oversee COVID-19 patients. Serious cases frequently had to be evacuated to urban centers due to the lack of healthcare facilities and medical personnel.

ii. Economic Impact

Supply chain interruptions and lockdowns had a significant negative impact on villagers, especially those who depended on agriculture and informal labour. Increased levels of poverty and food insecurity were caused by the loss of jobs and income. Migrant workers risked unemployment and uncertainty when they returned to their villages.

iii. Education Disruption

Students in remote locations, where access to the internet and digital devices is constrained, faced a tremendous problem as a result of school closures and the move to online learning. Many pupils struggled to finish their education, particularly those who lived in isolated areas.

iv. Digital Divide

The pandemic brought attention to India's digital divide, which is reflected in rural areas' limited access to the internet and digital devices. During the crisis, this gap made it difficult to acquire information, healthcare, and education.

v. Agriculture

A vital function and continued throughout lockdowns, farmers' access to markets and the supply chain are affected by the pandemic. Their means of subsistence and income were impacted.

vi. Mental Health

The pressures of the epidemic, including disease, job loss, and social isolation, had a negative impact on the rural area's mental health. Rural communities have limited access to mental health care, and overcoming the stigma attached to mental health problems is still difficult.

vii. Social and Cultural Impact

Social segregation and lockout procedures shattered rural communities' customary social and cultural norms. The social fabric of these communities was affected by the reduction of social gatherings, religious occasions, and festivals.

viii. Distribution of Vaccines

Maintaining the cold chain and ensuring equal distribution are logistical issues throughout the launch of vaccines in remote areas. Issues with vaccination hesitancy and awareness also need to be addressed.

IV. Uses of Digital Security and Implementation in Post-Pandemic

Digital security is the process of preventing unauthorized access to, theft of, or damage to digital equipment, networks, and data. As more individuals work remotely and rely on digital technology for communication and healthcare services during the COVID-19 pandemic, digital security has become more crucial. The sub-sections are explained with a few examples of how COVID-19 employs digital security including;

A. Cybersecurity Attacks during Crisis

Cybersecurity attacks during crisis describe how there is a higher chance of cyber threats, like phishing, hacking, and data breaches, happening during emergencies or times of crisis. Cybercriminals frequently take advantage of these crises, like natural disasters or worldwide pandemics, to target companies, exploit weaknesses, and interfere with vital systems. To safeguard confidential data and preserve operational integrity during these periods, it is imperative to exercise vigilance and put strong cybersecurity measures in place. The organizations under stress are more susceptible to cybersecurity threats. COVID-19 pandemic has shown the crises raise the risk to digital security.

B. Enhancing Healthcare and Reducing Virus Transmission through Digital Technology

To deliver healthcare services, track the transmission of the virus, and provide assistance and medical consultations which are deployed by digital technologies. During the pandemic, digital technology was implemented in sturdier healthcare systems than in weaker and more vulnerable ones.

C. Digital Tools for Early COVID-19 Intervention

The control of COVID-19 was strongly correlated with early intervention using digital tools. A range of digital tools, including telemedicine, AI, contact tracing apps, and data analytics, are available for early COVID-19 intervention. These tools are used to manage vaccine distribution, facilitate remote medical consultations, track and mitigate the virus's spread, and quickly disseminate information. During the pandemic, they are essential to early detection, effective response, and public health safety.

D. Enterprises using Digital Transformation

To defend themselves against cyberattacks, businesses have implemented digital transformation in response to the COVID-19 pandemic. Enhancing endpoint security, putting in place a Zero Trust framework, fortifying cloud security, utilizing AI and sophisticated authentication techniques, raising staff security awareness, and guaranteeing regulatory compliance are all part of this. Taken together, these steps assist organizations in strengthening their defenses in the post-COVID-19 era.

E. Enhancement in Cyber-Attacks Sophistication

Cyber-attacks have evolved in sophistication in the post-COVID-19 era. Focus on cybersecurity training, sophisticated detection, robust endpoint security, timely patching, multi-factor authentication, network segmentation, and effective incident response and backup plans to defend against impending threats. Managing third-party risks, cooperating for threat intelligence, and adhering to regulations are all essential in the continuous fight against changing cyber threats.

V. Digital Security Impacts during Pre and Post Pandemic: A Comparative Study

In 2023, the environment has undergone a significant change as a result of the COVID-19 pandemic. Nowadays, cybercriminals have more access to resources and appreciation for the global movement towards remote work and increased reliance on digital technologies. Surprisingly, the statistics show that cyber-attacks have inclined into alarming information is shown as the evolution of cybersecurity trends from 2017 to 2023 as given in Table I.

Table I: Evolution of Cybersecurity Trends (2017-2023)

Category	*Before COVID (2017-2018)*	*During COVID (2019-2021)*	*After COVID (2022-2023)*
Cybersecurity Trends	Cyber-attacks were a growing concern but not yet a pandemic.	Cyber-attacks surged due to remote work and increased reliance on digital technologies.	Cyber-attacks remain a significant threat, with ongoing risks and vulnerabilities.
Statistics	Internet of Things (IoT) cyber-attacks are predicted to increase.	125% global increase in cyberattacks in 2021. - 358% increase in malware attacks in 2020.	Cybercrime affected over 53 million Americans in the first half of 2022.
Financial Impact	Data breaches had financial consequences but were not widespread.	Data breaches led to lost data, business interruptions, and revenue losses.	Affected organizations were reluctant to increase security spending.
Supply Chain Attacks	Supply chain attacks were emerging as a significant threat.	Cybercriminals targeted third-party suppliers to infiltrate client networks.	Supply chain attacks continue to pose risks that organizations must actively control.
Global Impact	Poorer nations faced increased cyber threats with ICT expansion.	Developing nations needed to identify and prevent cyber dangers.	Developing nations face cybersecurity challenges due to increased ICT use.
Government Strategies	Governments enhanced digital transformation strategies.	National digital strategies are in place, including AI, blockchain, and 5G.	Governments are focusing on emerging technologies and setting strategic directions.
Digital Innovation	Digital innovation was a driver of new business models.	Digital technologies strengthened research systems during the pandemic.	Technologies are used with consideration of privacy, security, and consumer protection.
Inclusive Digital Future	Pre-pandemic policies needed adjustments for inclusivity.	The pandemic underscored the need for a coordinated digital policy approach.	OECD Going Digital Integrated Policy Framework emphasizes inclusivity in digital transformation.

In the years leading up to the COVID-19 pandemic (2017-2018), cyber-attacks were a growing concern, with predictions of increasing IoT cyberattacks, however, not yet reached the pandemic scale. During the pandemic (2019-2021), the world witnessed a surge in cyberattacks due to the widespread adoption of remote work and increased reliance on digital technologies. This period saw a dramatic 125% global increase in cyberattacks, along with a substantial 358% rise in malware attacks. Data breaches became financially costly, causing lost data, business interruptions, and revenue losses. A notable trend emerged in supply chain attacks, where cybercriminals deliberately targeted third-party suppliers to infiltrate client networks. These trends continued into the post-pandemic era (2022-2023), with cyberattacks remaining a significant threat. Organizations faced ongoing risks and vulnerabilities, yet some were reluctant to increase security spending. Developing nations also grappled with cybersecurity challenges due to increased Information and Communication Technology, (ICT) use. Governments across the globe strengthened their digital transformation strategies and focused on emerging technologies such as AI, blockchain, and 5G (Generation). The Organisation for Economic Co-operation and Development (OECD) describes the Digital Integrated Policy Framework underscoring the importance of inclusivity in digital transformation, emphasizing the need for coordinated policies to navigate the evolving digital landscape.

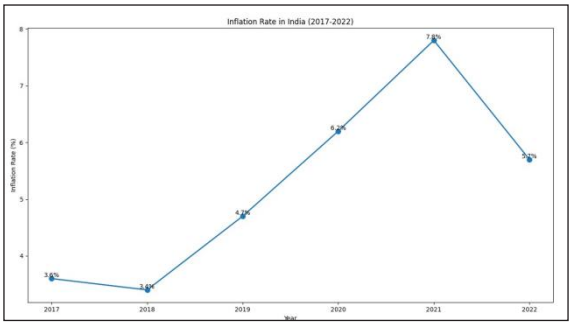

Fig. 2: Inflation Data in India

Fig. 2 shows the inflation rate in India from 2017 to 2023. The inflation rate was relatively low in the pre-COVID period (2017-2019), but it started to increase in 2020. The inflation rate peaked in April 2022 at 7.8%, but it has since declined to 5.7% in December 2022.

VI. Result and Discussion

In this work, Fig. 3 shows the size of abstract topic clusters monthly basis. In this work, three hues stand for distinct

categories used to categorize cyber threats: news, advertisement, and information.The graph illustrates how abstract topic cluster sizes change from month to month. There are a few big clusters in some months and a lot of small clusters in others. This implies that the year-round distribution of cyber threats is not uniform. Also, in cyber threats, the graph demonstrates classification schemes for cyber threats that are not exclusive of one another. Many cyber threats are categorized as both news and information in certain months. It indicates a temporal variation in the scope and complexity of cyber threats to develop preventative and remediation strategies to add aided information. This result shows that people are more likely to be online and socialize during these months as shown in Fig. 4 as well as July, August, and December tend to have smaller cluster sizes overall. This could be because people are less likely to be online and more likely to be on vacation during these months. As demonstrated in January, March, and May typically have higher percentages of cyber threats that are categorized as information. In general, the percentage of cyber threats that are categorized as news is higher in July, August, and December. This might be because people are more likely to read news articles online during these months. Across all months, the percentage of cyber threats categorized as advertisements is typically lower as demonstrated.

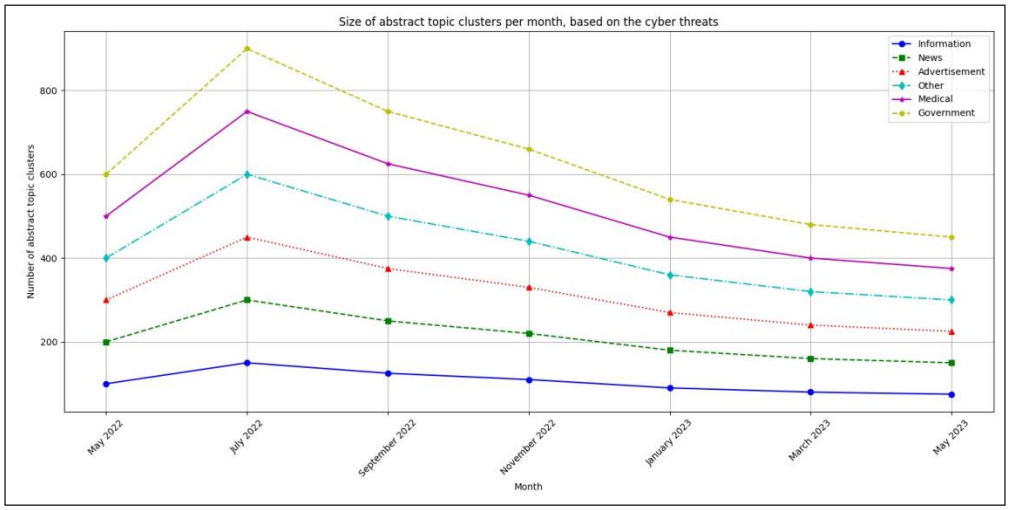

Fig. 3: Size of Abstract Topic Clusters Per Month, Based on the Cyber Threats

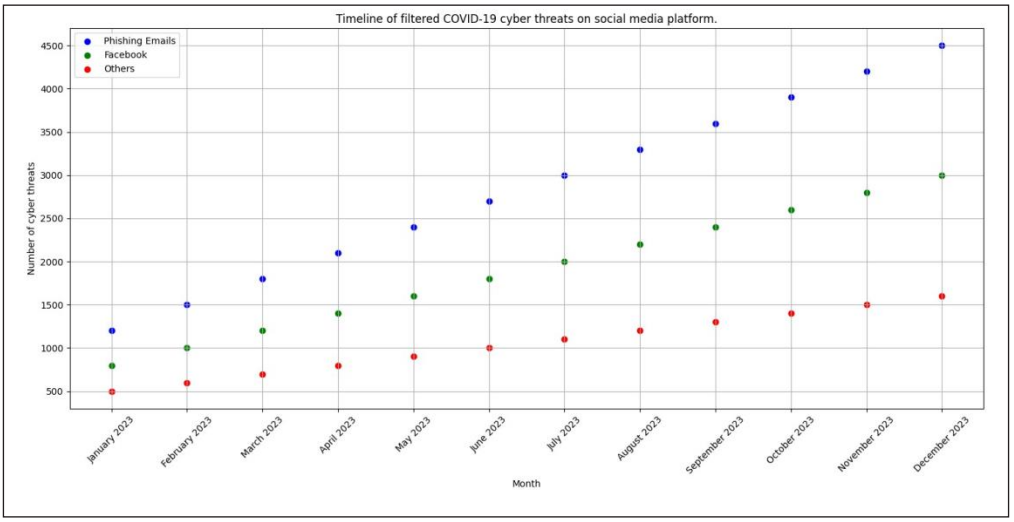

Fig. 4: Timeline of Filtered COVID-19 Cyber Threats on Social Media Platform

VII. Conclusion

In summary, this study emphasizes how critical digital security is, especially when it comes to immediate cybersecurity for remote workstations and long-term threat defence. It emphasizes the necessity of a thorough strategy that includes precautions like virtual private network (VPNs), encryption, and training to secure remote work settings. It is recognized that ransomware poses a growing risk to remote workers improving collaboration tool security and thwarting phishing attempts are

important. It is crucial to use cutting-edge technologies, like AI and machine learning for intrusion detection, automated security procedures, and flexibility in the face of changing threats. Furthermore, considering the world at large is recommended as a proactive measure to strengthen digital security in the post-COVID-19 era of increased digital activity and possible threats. It is imperative to use cutting-edge digital security to safeguard against impending cyber threats in the wake of COVID-19. This entails defending against new threats like ransomware, managing risks associated with home networks and personal devices, and protecting remote work environments. Utilizing AI and machine learning technologies improves security by automating procedures and responding to changing threats. In the post-pandemic digital environment, bolstering digital security requires a proactive, worldwide strategy.

References

[1] S. Hakak, W. Z. Khan, M. Imran, K. K. R. Choo, and M. Shoaib, "Have you been a victim of COVID-19 - Related cyber incidents?," *Survey, Taxonomy, and Mitigation Strategies*, *IEEE Access,* vol. 8, pp. 124134-124144, 2020.

[2] C. Sohrabi, Z. Alsafi, N. O'Neill, M. Khan, A. Kerwan, A. Al-Jabir, C. Iosifidis, and R. Agha, "World Health Organization declares global emergency: A review of the 2019 novel coronavirus (COVID-19)," *International Journal of Surgery*, vol. 76, pp. 71-76, Apr. 2020.

[3] S. O. Cheng, and S. Khan, "Europe's response to COVID-19 in March and April 2020 - A letter to the editor on 'World Health Organization' declares global emergency: A review of the 2019 novel coronavirus (COVID-19)," *International Journal of Surgery*, vol. 78, no. 3-4, Jun. 2020.

[4] A. Liu, "Philanthropy and humanity in the face of a pandemic - A letter to the editor on 'World Health Organization' declares global emergency: A review 2019 novel coronavirus (COVID-19)," *International Journal of Surgery,* vol. 76, no. 10, pp. 71-76, Jul. 2020.

[5] Y. Ali, M. Alradhawi, N. Shubber, and A. R. Abbas, "Personal protective equipment in the response to the SARS-CoV-2 outbreak - A letter to the editor on 'World Health Organization' declares global emergency: A review of the 2019 novel coronavirus (COVID-19)," *International Journal of Surgery,* vol. 78, pp. 66-67, Jun. 2020.

[6] B. Tabisula, and C. Uwaoma, "The need for an adaptive sociotechnical model for managing mental health in a pandemic," in *2022* IEEE *International Conference on Digital Health (ICDH),* Barcelona, Spain, 2022, pp. 66-68.

[7] K. Halouzka, A. Coufalíková, L. Buřita, and P. Kozak, "The impact of the COVID-19 pandemic on the evolution of cyber threats," *International Conference on Military Technologies,* Brno, Czech Republic, 2023, pp. 1-8.

[8] M. Imran, S. Hakak, W. Z. Khan, K.-K. R. Choo, and M. Shoaib, "Have you experienced a cyber incident related to COVID-19? Survey, classification, and prevention measures," *IEEE Access*, vol. 8, pp. 124134-124144, 2020.

[9] K. Parti, J. Hawdon, and T. E. Dearden, "American cybercrime in the midst of COVID-19: Preliminary findings from a natural experiment," *Am. J. Crim. Justice*, pp. 1-17, 2020.

[10] R. Sharma, and N. Sawant, "Cybersecurity during COVID-19: Challenges and countermeasures," in *Cybersecurity in COVID-19 Era*, Springer, pp. 11-23, 2021.

[11] A. Khan, A. Singh, and A. Kanwar, "The rise of cybersecurity threats during COVID-19: A study on India," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, pp. 144-151, 2021.

[12] K. Kapoor, and M. P. Gupta, "Impact of COVID-19 pandemic on cybersecurity: A study with reference to India," *International Journal of Computer Applications,* vol. 179, no. 13, pp. 30-36, 2021.

[13] S. Choudhury, and K. C. Dey, "Emerging cybersecurity threats during COVID-19 pandemic: The case of India," *International Journal of Criminal Justice Sciences,* vol. 15, no. 1, pp. 1307-1320, 2020.

[14] S. Gupta, and V. Gupta, "Cyber security challenges during COVID-19 in India," in *The Impact of the COVID-19 Pandemic on Business and Industry,* Springer, 2021, pp. 131-143.

[15] M. Singh, and S. Bhatia, "Cyber threats in India during COVID-19 and mitigation strategies," *Journal of Information Security and Applications,* vol. 62, p. 102712, 2021.

[16] A. Khurshid, "Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic," *JMIR Medical Informatics,* vol. 8, p. e20477, Springer, 2021.

[17] S. M. Badawy, and A. Radovic, "Digital approaches to remote pediatric health care delivery during the COVID-19 pandemic: Existing evidence and a call for further research," *JMIR Pediatrics and Parenting,* vol. 3, p. e20049, 2020.

[18] A. Sardi, A. Rizzi, and E. Sorano, "Cyber risk in health facilities: A systematic literature review," *Sustainability*, vol. 12, p. 7002, 2020.

[19] M. Z. Ahmed, O. Ahmed, Z. Aibao, S. Hanbin, L. Siyu, and A. Ahmad, "Epidemic of COVID-19 in China and associated psychological problems," *Asian Journal of Psychiatry*, vol. 51, pp. 102092-102092, 2020.

[20] H-W. Zhang, J. Yu, H-J. Xu, Y. Lei, Z-H. Pu, and W-C. Dai, "Coronavirus international public health emergencies: Implications for radiology management," *Academic Radiology*, vol. 27, no. 4, pp. 463-467, 2020.

[21] Y. Zhao, S. Cheng, X. Yu, and H. Xu, "Chinese public's attention to the COVID-19 epidemic on social media: Observational descriptive study," *Journal of Medical Internet Research*, vol. 22, no. 5, p. e18825, 2020.

[22] L. Lu, W. Xiong, D. Liu, J. Liu, D. Yang, and N. Li, "New onset acute symptomatic seizure and risk factors in coronavirus disease 2019: A retrospective multicenter study," *Epilepsia*, vol. 61, no. 6, pp. e49-e53, 2020.

[23] L. O. Olagoke, and A. E. Topcu, "Characterizing the effectiveness of COVID-19 mitigation measures: A data-centric approach," in *46th International Conference on Telecommunications and Signal Processing*, Prague, Czech Republic, 2023, pp. 254-259.

[24] K. Ewaldo, I. G. B. G. B. Abadi, P. K. Chekitana, and R. Sari, "The e-learning effect on learning activities during COVID-19 pandemic in higher education," in *2022 International Conference on Information Management and Technology (ICIMTech),* Semarang, Indonesia, 2022, pp. 589-593, doi: https://doi.org/10.1109/ICIMTech55957.2022.9915138.

[25] S. Kumar, M. S. Gaur, P. Sagar Sharma, and V. Sagar, "Post pandemic cyber attacks impacts and countermeasures: A systematic review," *International Conference on Artificial Intelligence and Smart Communication,* India, 2023, pp. 192-199.

[26] M. Sharma, and A. Kaul, "Suspicious permissions detection of COVID-19 themed malicious android applications," *IEEE 2nd International Conference on AI in Cybersecurity*, Houston, TX, USA, 2023, pp. 1-6.

[27] E. Viardot, A. Brem, and P. A. Nylund, "Post-pandemic implications for crisis innovation: A technological innovation view," *Technological Forecasting and Social Change,* vol. 194, p. 122680, 2023.

[28] V. Wylde, E. Prakash, C. Hewage, and J. Platts, "Post-COVID-19 metaverse cybersecurity and data privacy: Present and future challenges," *Data Protection in a Post-Pandemic Society*, Springer, Cham, 2023.

[29] R. Kumar, Siddharth, Chirag, and Nitish, "What changed in the cyber-security after COVID-19?," *Computers and Security,* vol. 120, p. 102821, 2022.

[30] L. Ali et al., "Post-Covid-19 pandemic IT project management skills and challenges," *International Conference on Business Analytics for Technology and Security,* Dubai, United Arab Emirates, 2023, pp. 1-8.